(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-523012
(P2004-523012A)
(43)公表日　平成16年7月29日(2004.7.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/00	G06F 13/00	610Q	5B085
G06F 15/00	G06F 15/00	330A	5K030
H04L 12/58	H04L 12/58	100F	

審査請求 有　予備審査請求 有　（全 46 頁）

(21)出願番号　特願2001-520583(P2001-520583)
(86)(22)出願日　平成12年8月25日(2000.8.25)
(85)翻訳文提出日　平成14年3月1日(2002.3.1)
(86)国際出願番号　PCT/US2000/023561
(87)国際公開番号　WO2001/016695
(87)国際公開日　平成13年3月8日(2001.3.8)
(31)優先権主張番号　60/152,025
(32)優先日　平成11年9月1日(1999.9.1)
(33)優先権主張国　米国(US)
(31)優先権主張番号　60/180,937
(32)優先日　平成12年2月8日(2000.2.8)
(33)優先権主張国　米国(US)

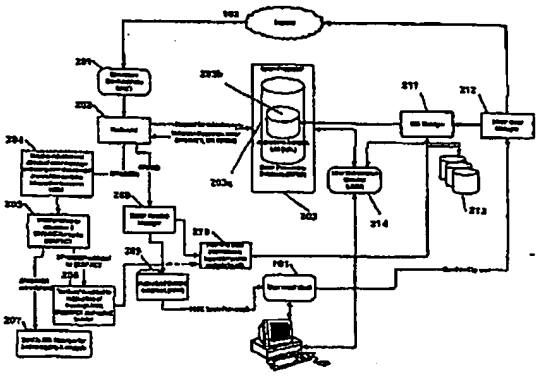
(71)出願人　502075940
カツィカス，　ピーター，　エル．
アメリカ合衆国　ハワイ州　ホノルル　ウッドローン　ドライブ　２８００　スイート　２４５
(74)代理人　100085028
弁理士　西森　浩司
(72)発明者　カツィカス，　ピーター，　エル．
アメリカ合衆国　ハワイ州　ホノルル　ウッドローン　ドライブ　２８００　スイート　２４５

Fターム(参考)　5B085 AA08 AE00
5K030 GA15 HA06 HD10 KA07 KX24 LC15

最終頁に続く

(54)【発明の名称】権限が与えられていない電子メールを排除するシステム

(57)【要約】
【課題】ネットワークでユーザに送信された権限が与えられていない電子メールを排除するシステム
【解決手段】ネットワークでユーザに送信された権限が与えられていない電子メールを排除するシステムは、ネットワークとユーザに送信された電子メールを受信するユーザの電子メールクライアント（１０１）との間に接続された電子メール受信サーバ（１０４）を備え、送信者のアドレスが「権限が与えられた送信者」リスト（ＡＳＬリスト）に保存されているどの送信者のアドレスにも一致しないような電子メールを拒絶するようになっている。ＡＳＬリストは、スパム処理モジュールと共に使用可能なＡＳＬデータベース（２０３ａ）の中のＡＳＬマネージャ（２１１）に保存される。リダイレクタモジュール（２０２）は、確認の要求をスパム処理モジュールに送信することに関して、送信者のアドレスがＡＳＬリストのどの権限が与えられた送信者アドレスにも一致しない場合にはその電子メールを拒絶する。リダイレクタモジュールによって拒絶された電子メールは、ウェブ



【特許請求の範囲】
【請求項１】
ネットワークと電子メールクライアント（１０１）の間に接続された電子メール受信サーバ（１０４）と共に作動可能であり、ネットワーク上でユーザへ送信された権限が与えられていない電子メールを排除し、ユーザのユニークな電子メールアドレスへアドレス指定された電子メールを受信するためのシステムにおいて、
（ａ）ユーザへ電子メールを送信する権限が与えられた送信者の電子メールアドレスのＡＳＬリスト（２０３ｂ）を維持する、権限が与えられた送信者リスト（ＡＳＬ）モジュール（２０３、２１１）を有する電子メール受信サーバと、
（ｂ）送信者の電子メールアドレスがユーザのためのＡＳＬリスト上に維持されていない場合、ユーザの電子メールアドレスへアドレス指定された電子メールの受信を拒絶するための前記ＡＳＬモジュール（２０３）と共に作動可能な電子メール拒絶モジュール（２０２）と、
を備えたことを特徴とするシステム。
【請求項２】
前記ＡＳＬモジュールが、システムの各加入者のために権限が与えられた送信者アドレスのＡＳＬリストを保存しているＡＳＬデータベース（２０３ｂ）と、
一致に関しＡＳＬリストを検査するためのスパム処理モジュール（２０３）と、
そして、
ＡＳＬリストを作成し、維持し、更新するＡＳＬマネージャ（２１１）と、
を含む請求項１に記載のシステム。
【請求項３】
前記電子メール拒絶モジュール（２０２）が、送信者の送信元アドレスを示し、受信者の送信先アドレスが示された電子メール送信メッセージを受信し、送信者の送信元アドレスが予定する受信者の送信先アドレスと対応するＡＳＬリスト上に維持された権限が与えられた送信者アドレスとが一致するかどうかを判断するために、スパムプロセッサモジュールへ確認の要求を送り、権限が与えられた送信者アドレスとの一致が見つかった場合には、電子メールを受信し、権限が与えられた送信者アドレスとの一致がＡＳＬリスト上に見つからなかった場合には、電子メールを拒絶する請求項２に記載のシステム。
【請求項４】
拒絶された電子メールが転送され、送信者が予定する受信者にとって電子メールの正当な送信者であることを確認するために、送信者のアドレスへメッセージを送信するウェブベースメッセージ（ＷＢＭ）モジュールをさらに含む請求項３に記載のシステム。
【請求項５】
前記ＷＢＭモジュールが、通知された送信者がログオンし、人にしか実行できない相互対話処理を経て、送信者が電子メールの正当な送信者であることを確認することができる別のウェブサイトを含む請求項４に記載のシステム。
【請求項６】
前記相互対話処理が、非標準的なフォントで表されるワードのグラフィックイメージのディスプレイと、ユーザがそのワードのグラフィックイメージに対応するワードの入力を含むことによって相互対話処理が機械的なプログラムによって実行されないことを確認するようになっている請求項５に記載のシステム。
【請求項７】
送信者が、予定された受信者ユーザにとって電子メールの正当な送信者であると一旦確認されると、その電子メールがリダイレクタモジュールに拒絶されながらもＷＢＭモジュールに正当であるとして確認されたと示すコードと共に、前記ＷＢＭモジュールが電子メールユーザの電子メールボックスへ電子メールを送信する請求項４に記載のシステム。
【請求項８】
電子メールクライアントから送信された電子メールの送信元／送信先アドレスを得て、の

項３に記載のシステム。
【請求項９】
電子メールクライアントから送信された電子メールの送信元／送信先アドレスを得て、のちの分析のためにＡＳＬマネージャへ送信する電子メール送信マネージャを更に含む請求項２に記載のシステム。
【請求項１０】
ＡＳＬマネージャが、受信メールと、送信メールと、電子メールクライアントに関する電子メールサービス機能へのユーザ入力と、ウェブサイトのユーザブラウザからの入力と、ユーザデスクトップオーガナイザーと、他のコンタクトリストと、サード・パーティのアドレスプログラム入力からなる電子メールアドレスソースの群から選択した一つの電子メールアドレスソースより得たデータを使用するＡＳＬリストを更新する、予め定めたアドレス収集ルールを処理するためのルールプロセッサを含む請求項２に記載のシステム。
【請求項１１】
ＡＳＬマネージャが、ユーザ電子メール登録分析と、有効期限分析と、低／高電子メール容量分析と、ファジーロジック分析と、サード・パーティのデータ分析からなる分析群から選択した一つの分析ソースより得たデータを使用するＡＳＬリストを更新する、予め定めた分析ルールを処理するために、ルールプロセッサを維持する請求項２に記載のシステム。
【請求項１２】
ＡＳＬマネージャが、フレンドとしていつも権限が与えられたステータスと、日付の範囲内でフレンドとして権限が与えられたステータスと、有効期限以前にフレンドとして権限が与えられたステータスと、スパマーとしていつも拒絶されたステータスと、ブラックリストと一致するスパマーとして拒絶されたステータスと、エラーメッセージとともに送信されたスパマーとして拒絶されたステータスからなる送信者アドレスステータスの群から選択した一つの送信者アドレスステータスを示すＡＳＬリストを維持する請求項２に記載のシステム。
【請求項１３】
（ａ）ユーザへ電子メールを送信する権限が与えられた、外部ユーザの電子メールアドレスの権限が与えられた送信者リスト（ＡＳＬリスト）を維持し、
（ｂ）送信者の電子メールアドレスがユーザのためにＡＳＬリスト上に維持されていない場合、ユーザの電子メールアドレスへ送信された電子メールの受信を拒絶する、
ことを特徴とするユーザのユニークな電子メールアドレスへアドレス指定され、ネットワーク上でユーザへ送信された権限が与えられていない電子メールを排除する方法。
【請求項１４】
送信者が電子メールの正当な送信者であると確認するために送信者を通知するメッセージを予定された受信者へ送信するために、拒絶された電子メールをウェブサイトへ転送することをさらに特徴とする請求項１３に記載の方法。
【請求項１５】
ウェブサイトで、通知された送信者とともに、人にしかできない相互対話処理を実行することをさらに特徴とする請求項１４に記載の方法。
【請求項１６】
ＡＳＬリストを維持することが、受信メール、送信メール、電子メールサービス機能へのユーザ入力、ウェブサイトのユーザブラウザからの入力、ユーザデスクトップオーガナイザーと他のコンタクトリスト、サード・パーティのアドレスプログラム入力といったソースのいずれから得られるデータを用いてＡＳＬリストを更新することを含む請求項１３に記載の方法。
【請求項１７】
ＡＳＬリストを維持することが、ユーザ電子メール登録分析、有効期限分析、低／高電子メール容量分析、ファジーロジック分析、サード・パーティのデータ分析といった要素の

3に記載の方法。
【請求項１８】
ネットワークを通じて送信され、ユニークな電子メールアドレスへアドレス指定された権限が与えられていない電子メールを、システムのユーザのために排除する電子メールサーバシステムにおいて、
（ａ）ユーザへ電子メールを送信する権限が与えられた送信者の電子メールアドレスのＡＳＬリストを維持する権限が与えられた送信者リスト（ＡＳＬ）モジュール（２０３、２１１）と、
（ｂ）ユーザの電子メールアドレスへアドレス指定された電子メールの受信者を拒絶する前記ＡＳＬモジュールと共に作動可能な電子メール拒絶モジュール（２０２）と、
有して構成されたことを特徴とする電子メールサーバシステム。
【請求項１９】
前記ＡＳＬモジュールは、システムの各加入者のために、権限が与えられた送信者アドレスのＡＳＬリストとを保存するＡＳＬデータベース、一致に関してＡＳＬリストを検査するスパムプロセッサモジュール、ＡＳＬリストを作成し、維持し、更新するＡＳＬマネージャを含む請求項１９に記載の電子メールサーバシステム。
【請求項２０】
送信者の送信元アドレスを示し、受信者の送信先アドレスが示された電子メール送信メッセージを受信し、送信者の送信元アドレスが予定された受信者の送信先アドレスと対応するＡＳＬリスト上で維持された権限が与えられた送信者アドレスとが一致するかどうかを判断するために、スパムプロセッサモジュールへ確認の要求を送り、権限が与えられた送信者アドレスとの一致が見つかった場合には、電子メールを受信し、権限が与えられた送信者アドレスとの一致がＡＳＬリスト上に見つからなかった場合には、電子メールを拒絶する電子メール拒絶モジュールをさらに有していることを特徴とする請求項１９に記載の電子メールサーバシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、望まない電子メールを排除するためのシステムに関し、特に、電子メールが受理されるために権限が与えられた送信者によって送信されたと全ての電子メールを識別しなければならないシステムに関する。
【０００２】
【従来の技術】
求めていない電子メール又は権限が与えられていない電子メール（例えば、迷惑メール）は、現在の公共のインターネットといった世界的なネットワークのユーザにとって重大な悩みの種である。一度ネットワークシステムにおいてある人の電子メールアドレスが知られると、それはコンピュータ処理されたリストの中で容易にコピーされ、そして、そのユーザに対して電子メールを送信する権限が与えられていないか又は望まれていない無制限の人々に電子的に送信されうる。
【０００３】
ユーザの電子メールボックスには、そのような権限が与えられていない電子メールが殺到しうる。権限が与えられていない又は求めていない電子メールは、一般的に産業界において「スパム」という言葉で呼ばれているが、その言葉はホーメル社が「Ｓｐａｍ」という商標で販売している人気のある肉の缶詰製品を連想させ又はけなすものではない。ユーザは、商業情報サービスプロバイダ（ＩＳＰ）サービスに所定の電子メールアドレスを持っているであろうが、プロバイダのサービスは受け入れ及び／又は記憶可能な電子メールの量を制限するか、または受信した量によってユーザに課金する。ユーザは、同様に、そのような求めていない電子メールを開き、そして再び見ることで重要な時間を無駄に使うことになる。権限が与えられていない電子メールは、同様に、ユーザのコンピューターシス

が権限が与えられていないポイントとして使用することができるウィルス又は有害なソフトウェアエージェントを電子メールの中に同封するような無節操な人によって送信されるだろう。

【０００４】

【発明が解決しようとする課題】

スパムの受信を管理するための現代のソフトウェアの全て、そうでない場合はそのほとんどが、公知のスパムのソースあるいはスパムの送信者（スパマー）の確認リストを使用することを基礎としている。かかる従来のスパム管理ソフトウェアは、送信者が除外リストにあると識別されず、電子メールがフィルタを通過できれば全ての電子メールを正当であるとして受信することに基づき動作する。

【０００５】

この方法は、単に確認リストととしては良好であるが、ユーザがスパムを受信しないということは保証はできない。スパマーリストは頻繁に更新されなければならず、全ての加入者へタイムリーな方法でスパム管理ソフトウェアあるいはサービスを配信しなければならない。慣れたスパマーは、頻繁に彼らのソースインターネットアドレスを変更し、そして、除外リストを最新のものに保とうとする試みを破ることができる。彼らは、同様に、害が無いとして通過できるか、あるいは広く認められた名前の電子メールのソースを偽装するために他の組織のインターネットサーバを通じて求めていない電子メールを送信することができる。ユーザの電子メールアドレスも公共のチャットルームあるいは公共の掲示板で多くの人々に知られることになる。個人による電子メールの送信は技術的にスパムでないため、個人から送信された求めていない電子メールはスパマーリスト上に足跡を残さない。

【０００６】

従って、本発明の第一の目的は、ソースアドレスを頻繁に変更し、または、他のサーバを通じて電子メールを送信してそれらを偽装するスパマーによって、あるいは、ユーザが要求せず又は認可していない電子メールを個人が送信することによって破ることのできないスパム管理システムを提供することにある。特に本発明の目的は、送信者がユーザの受け入れリストに存在すると認められないかぎり全電子メールを権限が与えられていないとして本発明のシステムが拒絶することにある。

【０００７】

【課題を解決するための手段】

本発明に従い、ネットワークにおいてユーザに送信された権限が与えられていない電子メールを排除するシステムは、

（ａ）ユーザの特定の電子メールアドレスへアドレス指定され、ネットワークを通じて送信された電子メールの受信をユーザに配信するための電子メールクライアントと、

（ｂ）ネットワークとユーザの特定の電子メールアドレスへアドレス指定された電子メールを受信するための電子メールクライアントとの間に接続された電子メール受信サーバであって、ユーザへ電子メールを送信する権限が与えられた外部ユーザの電子メールアドレスのＡＳＬリストを保存した権限が与えられた送信者リスト（ＡＳＬ）モジュールを有する上記電子メール受信サーバと、

（ｃ）送信者の電子メールアドレスがユーザのためのＡＳＬリストに保存されていないものである場合には、ユーザの電子メールアドレスに送信された電子メールの受信を拒絶するための、ＡＳＬモジュールと共に作動可能な電子メール拒絶モジュールとを含む。

【０００８】

好ましい実施形態において、システムのＡＳＬモジュールは、システムの各加入者のために権限が与えられた送信者アドレスのＡＳＬリストを保存するためのＡＳＬデータベースと、一致がないかどうかＡＳＬリストを照合するためのスパムプロセッサモジュールと、そして、ＡＳＬリストを作成し、維持し、最新のものにするためのＡＳＬマネージャとを含む。リダイレクタモジュールは、確認の要求をスパム処理モジュールに送信することに

者アドレスとも一致しない場合には、電子メールを拒絶する。リダイレクタモジュールによって拒絶された電子メールは、ウェブベースメッセージングモジュール（ＷＢＭ）に転送され、このモジュールは送信者が受信者に対する正当な電子メール送信者であることを確認するために送信者に通知するメッセージを送信する。もし送信者がステータスを確認するためにログオンするならば、ＷＢＭモジュールは、確認行為が機械的なプログラムによって行なわれないことを確認するため、人間だけが行なうことのできる相互対話手続きを実行する。ＡＳＬマネージャは、送信された電子メール、受信された電子メール、ユーザによって保存されたコンタクトリスト、ユーザ優先入力、サード・パーティのプログラム等を含む様々な電子メール利用ソースの分析から収集された送信者アドレスのデータに基づいたＡＳＬリストを管理する。

【０００９】

本発明は、上記機能を実行するための関連する方法のみならず、上記のこれらの機能を実行できるようにするソフトウェア構成要素を含む。

【００１０】

【発明の実施の形態】

以下、図面を参照し、本発明の他の目的、特徴、及び利点について以下に詳細に説明する。

【００１１】

権限が与えられていないとして除外リストに記載された場合を除いて、全電子メールを受信する既存のスパム管理方法のアプローチとは異なり、本発明の基本的な原理は、権限が与えられたとして包含リストにリストアップされていなければ全電子メールを拒絶することである。この様に、ユーザが求めていない電子メールを送信する個人と同様に、認められていないスパマーから送信された電子メールを排除することが可能である。公知の電子メールフィルタリングシステムと異なり、本発明は、求めていない電子メールを、それが受信された後に排除しようとはしない。それどころか、それは、最も早いエントリーレベルでその電子メールを完全に拒絶する。こうして、本発明は、ユーザが電子メールを受信するために、送信者が「権限が与えられた送信者」リスト上に発見されなければ、権限が与えられていないとして全電子メールを扱うとい前提で実施される。このことは、スパム送信者が即座に自分たちのソースアドレスあるいは見かけのアイデンティティを変更することができ、そして公共の場での個人が、他のユーザの電子メールアドレスを入手し、彼らに求めていない電子メールを送信することができる環境内で、本来強力で１００％有効なスパム管理解決法を提供する。

【００１２】

以下は、本発明の概念を実行するためのシステムにおける一つの好ましい実施例の詳細な説明である。この実施例では、スパム管理システムは、誰にどれだけの頻度で送信電子メールが他のユーザにアドレスされたかというようなユーザの電子メールの使用に関する継続した分析を基礎とし、ユーザの知られたコンタクトやユーザによって維持されそして権限が与えられたとみなされた人々を示すリストあるいはファイルで確認される仲間というようなハイレベルなユーザコンタクトデータの収集により、「権限が与えられた送信者」のリストをインテリジェントに明確にする。「権限が与えられた送信者」のリストは、さらに、ユーザによって、権限が与えられた送信者を加えたり削除したりするように、任意の時間に最新のものにされ、処理されることになる。この特定の実現例を使用し説明する方法により協働して利用できるように所定の構成要素を提供し構成するが、本発明の完全な範囲は、以下説明する発明の概念に対する他の適当な変形例及び変更例を含むものであると理解すべきである。

【００１３】

図１Ａは、インターネット上において送信し受信される電子メールのための標準的な電子メールシステムのブロック図であり、スパマーからの電子メールを排除するための従来方法を説明するために使用される。そのシステムは、インターネット上において電子メール

的に選ばれたＩＳＰとともに、電子メールサービスを含むインターネットアクセスや関係するサービスに加入する。そのユーザは、ダイアルアップあるいは高速回線接続と標準的ブラウザを使用して、ＩＳＰを通してインターネットにアクセスする。ブラウザは、ワシントンのベルビューに本部を置くＭｉｃｒｏｓｏｆｔによって配布されたＯｕｔｌｏｏｋ（商標）電子メールクライアント、あるいはバージニアのフェアファックスに本部を置くＡＯＬ／Ｎｅｔｓｃａｐｅによって配布されたＮｅｔｓｃａｐｅ（商標）電子メールクライアントというような標準的な電子メールクライアント１０１を含み、これと共に機能する。ＩＳＰは、インターネット上で、ユーザによるアドレスが可能なドメインネームに対応するウェブサイトのアドレスで働く。ＩＳＰのサービス機能は、一つ以上のサーバを通して、多くの加入者に対して働く。一般に、電子メールサーバ１０２は、電子メールサービス機能を処理するために使用される。インターネットからＩＳＰへ送信された電子メールは、アドレスがＩＳＰの権限が与えられた加入者であるかどうかというような種々の管理機能が働くＳＭＴＰサーバ１０２ｂで受信され、そして、その電子メールは、インボックス１０２ａと呼ばれるユーザのために留保された格納スペースに置かれる。ユーザは、自分達の電子メールクライアントでそれぞれ電子メールを作成し、そしてインターネット上でメールを受信者へ発送するＩＳＰにおいて、ＳＭＴＰサーバ１０２ｂへそれをアップロードすることで、電子メールを送信することができる。

【００１４】

従来のスパム防止管理は、ＳＭＴＰサーバ及び／又は電子メールクライアントで、実現できた。多くのＩＳＰは、ＳＭＴＰサーバで知られたスパマーの除外リストを実行する。加えて、これらＩＳＰは、ユーザが知っているある送信者からの求めていない電子メールをユーザが一般に排除できるようにしている。例えば、ユーザの電子メールクライアントは、ＳＭＴＰサーバにより受信された電子メールがユーザのインボックスに入る前に電子メールを排除するようＳＭＴＰサーバに求めていない電子メールの送信者アドレスをユーザが入力出来るようにする排除機能を有する。さらに、独立系ソフトウェア会社は、ユーザの電子メールクライアントと共に働く精巧な電子メール処理プログラムを販売している。例えば、いくつかの処理プログラムは、受信された電子メールを項目のファイルフォルダに分類するための機能を有し、そして認められていない送信者からの電子メールは、「その他」あるいは「認められていない」ファイルフォルダに入れられる。

【００１５】

図１Ｂは、本発明に係るシステムの概念的な概観が示されている。従来と同様、標準的な電子メールクライアント１０１は、ＳＭＴＰサーバ１０４ｂとインボックス１０４ａを経由するインターネットへ電子メールを送信し、そしてそれらから電子メールを受信するための電子メールサーバ１０４に接続される。しかしながら、この変更された電子メールサーバ１０４では、権限が与えられた送信者リスト（ＡＳＬ）マネージャは、ブロック１０５に示されるように、ユーザによって送信された電子メールから受信者のメールアドレスを得、同様に、ブロック１０６に示されるようにユーザへ送信された電子メールから送信者のメールアドレスを得る。ＡＳＬマネージャは、得られた送信者メールアドレスと受信者メールアドレスを分析し、そしてメールアドレスを加えたりＡＳＬリストあるいはＡＳＬデータベースと呼ばれる「権限が与えられた送信者」リストからアドレスを排除したりするため、（以下の詳細で記述された）予め定義したあるルールを使用する。ブロック１０７で示されるように、他の全電子メールは「権限が与えられていない」ものとして拒絶する一方で、ＡＳＬリストは、ＡＳＬリスト上にある送信者からだけの電子メールを受信するため、そして受信された電子メールをユーザのインボックス１０４ａに入れるようＳＭＴＰサーバ１０４Ｂにより使用される。

【００１６】

図２を参照して本発明のスパム防止システムの操作上ステップへのフローを説明する。説明の中で用いるある用語を次のように定義する。

【００１７】

スパム：本発明のスパム管理システムの例

加入者：本発明のスパム管理システムを使用しているＩＳＰ電子メールサービスに加入する人
フレンド：加入者へ電子メールを送信するためにスパム管理システムによって権限が与えられた電子メール送信ソース
スパマー：加入者へ電子メールを送信することが認められない電子メールソースのことであり、このソースはマニュアルあるいはインターネットを通して大容量の電子メールを繰り返して送信するコンピュータ処理された電子メールリスト郵送プログラムを使用している未知否認知あるいは不正な当事者であると一般的に理解されている。
コンタクト：加入者の正当な通信者として、システムによって確認されてきた電子メール送信ソースは、システムによって加入者へ電子メールを送信することが認められる。
サスペクト：スパマーかコンタクトかのどちらかとしてまだ識別されていない電子メール送信ソース

【００１８】

インターネット（１０３）から送信された電子メールは、加入者のために、ブロック２０１内のスパムカプ電子メールアドレス（ＳＫＥ）と呼ばれるＩＳＰ電子メールアドレスへ送信される。受信された電子メールは、リダイレクタ２０２をまず通過しなければならない。レダイレクタ２０２は、権限が与えられた送信者リスト（ＡＳＬ）２０３ｂを含み、スパムデータベース（ＳＰＤＢ）２０３ａを維持するスパムプロセッサ２０３からの電子メールのための確認を求めるリクエストを送信しなければならない。ＳＰＤＢデータベースとＡＳＬリストは、スパムカプの中心となっているその理由は、それらは、システムの各加入者へ電子メールを送信する権限が与えられた人々のリストを包含するからである。スパムプロセッサ２０３は、電子メールの送信者アドレスがＡＳＬリスト上に権限が与えられていない、つまりスパマーであるか、またはＡＳＬリスト上で認可されているアドレス、すなわちフレンドであるかのいずれかの応答を送信する。もしスパマーであるとする応答であれば、ブロック２０４に示されているように、例えばアドレスに書かれたユーザが存在しないという標準的エラーメッセージが送信サーバへ送信されることで、リダイレクタ２０２は、その電子メールを拒絶する。

【００１９】

システムへの改良として、ブロック２０５にあるウェブベースメッセンジャー（ＷＢＭ）プロセスは、拒絶された電子メールが権限が与えられていないがＡＳＬリストにスパマーとして記載されていない人物からのものである場合には、補正手続を提供するためセットアップできる。その権限が与えられていない電子メールは、実際には、スパム防止システムにおいて以前に処理された人物からではなく、加入者へ到達する正当な理由を持つ人物からのものであろう。ＷＢＭプロセス２０５は、電子メールが転送されるスパム管理システムの一部としてセットアップされる。拒絶された電子メールの受信者に関して、ＷＢＭプロセスは、電子メールごとにそれぞれＩＤコードと有効期限を割り当てて、それをＷＢＭデータベース内に保管する。そしてＷＢＭプロセスは、今やサスペクトとして扱われるようになった電子メール送信者へ、エラー応答電子メールを送信する。例えば、エラーメッセージは次にとおりである：
「貴方が加入者のアドレスへ送信した電子メールは、スパム電子メールのソースたる権限が与えられていない送信者アドレスから送信されたものとして、このサイトに拒絶されました。もし貴方が、加入者に自分の電子メールを届ける正当な理由を有する人物である旨の証明をお望みであればＷＢＭサイトへ行き、コンタクトとして自分のステータスを確認して下さい。」

【００２０】

ＷＢＭは、サスペクトとの相互対話手続のため別々のウェブサイトアドレスを所有するか、あるいはサスペクトからの電子メール応答を受信し認識するためセットアップされる。あるサスペクトがエラー応答電子メールを受信した場合、かれらが加入者にとって正当なコンタクトであれば、正当なコンタクトとして自らを確認するため、ＷＢＭサイトへ行くまたは同等電子メールの送信を選択する。有効期限以前に行われたならば、ＷＢＭ

プロセスは、ブロック２０６に示されるように「コンタクト」のような特別なコードワードを転送された電子メールのサブジェクト欄に追加し、そして権限が与えられた送信者メールボックス（ＡＳＭ）２０９へ電子メールを再送信する。このプロセスを経て再転送された電子メールの送信者アドレスは、同様に保管され（ブロック２１０へ接続された回線によって示されるように）、ＡＳＬマネージャ２１１がサスペクトのステータスをフレンドへ格上げすべきか、そしてＡＳＬ２０３ｂへ追加するべきかを決定するというさらなる分析のために登録される。サスペクトが回答しない場合は、この事実も、さらなる分析のためＡＳＬマネージャへ送信される。スパマーは、バッチ電子メールを送信する際に自動プログラムを使用し、次に通常のＷＢＭサイトへログオンするため人間の応答時間をかけるか又は自らの正当なステータスを確認するために回答電子メールを送信するので追加確認ステップは有効にスパマーを排除できる。

【００２１】

送信者がフレンドであるという確認応答をスパムプロセッサが送信する場合は、リダイレクタ２０２は加入者のステータスを検査して加入者のインボックスであるＡＳＭ２０９に電子メールを保存するという管理機能が働くブロック２０８にあるようなＳＭＴＰ受信マネージャへ電子メールを送る。こうしてユーザは、（ＰＯＰ３あるいはＩＭＡＰ４のような標準的なインターネットプロトコルを使用している）ＡＳＭインボックスから、自分のコンピュータ上のユーザ電子メールクライアント１０１を通して、自分の電子メールを集めることができる。システムに権限が与えられたと認識されていない送信者からの全電子メールは拒絶されてしまっているので、ユーザの電子メールは１００％スパムから逃れられる。ＳＭＴＰ受信マネージャは、同様に、フレンドからの電子メールの受信情報を登録し、さらなる分析のためＡＳＬ２０３ｂへ電子メールを送信するようになっている。

【００２２】

ユーザは、標準的なＳＭＴＰプロトコル経由の電子メールクライアント１０１上で作成され送信された電子メールをＩＳＰの電子メールサーバへ送信する。ＩＳＰのＳＭＴＰサーバは、システム内の電子メールアドレスをユーザに提供し、ユーザの電子メールをスパムカプシステム内のインターネット上で受信者の電子メールアドレスへ送信する役割を有し、ＳＭＴＰ送信マネージャ２１２は、通常の電子メール送信プロセスに介入するように設けられている。ＳＭＴＰ送信マネージャ２１２は、全送信電子メールからヘッダ情報をコピーし、そのデータをＡＳＬマネージャ２１１へ送り、そして電子メールをその予定された目的地へ送信する。ＡＳＬマネージャ２１２は、本発明において鍵となる機能の一つを実行する。このマネージャは、送信された電子メールのヘッダと、電子メールログやユーザに供給されたリストのような、ＩＳＰ電子メールサーバシステムによって維持された他のデータソース２１３からのデータとを分析する。（以下のより詳細に説明する）その分析ルーチンに基づいて、ＡＳＬマネージャ２１１は、ＳＰＤＢデータベースとＡＳＬリストを検査し、ポピュレートし、そして電子メールアドレスと加入者へ電子メールを送信する権限が与えられた送信者に関する他のデータで更新する。スパムカプシステムも、ユーザ情報と相互に作用し合い、ユーザのためにスパムカプ電子メール操作を一層の改良するためスパムカプにその情報をアップロードするユーザ維持モジュール（ＵＭＭ）２１４を包含する。

【００２３】

図３Ａと図３Ｂには、標準的ＳＭＴＰ電子メール送信プロセス（従来技術）が、本発明に使用されている変更された電子メール送信プロセスと比較して示されている。図３Ａにあるように、標準的な電子メール送信プロセスでは、ユーザの電子メールクライアントからＩＳＰの電子メールサーバへ送信された電子メールは、正しいシンタックス、エイリアス拡大等の検査と受信者メールアドレス（おそらく一つ以上）リストを確認するための検査といった前処理がなされる。サーバ電子メールマネージャーは、順番に各受信者メールアドレスを入手し、目的地であるＳＭＴＰサーバとの接続を設定し、受信者の電子メールアドレスが正しいかどうかの証明を試みる。もし交渉に成功しなければ、エラーメッセージ

本文を目的地であるサーバへ送信し、適切な「クロース接続」（ｃｌｏｓｅ ｃｏｎｎｅｃｔｉｏｎ）操作を実行する。図３Ｂにあるように、本発明の変更された電子メール送信システムでは、クライアントから送信された電子メールは前処理され、受信者が確認され、目的地であるサーバとの接続が通常通り試みられる。成功している交渉に関して、スパムカプＳＭＴＰ送信マネージャ２１２は、成功した受信者電子メールアドレスをコピーし、ＡＳＬマネージャ２１１へそのデータを送る。加入者が電子メールを送信したことのあるどの人からの電子メールも受信することを加入者によって認可されるという前提に関して、加入者が電子メールを送信した人の適切な電子メールアドレスが、加入者へ電子メールを送信する権限が与えられた人のＡＳＬリストへ追加される。送信された電子メールデータは、たとえば、ある数以上の電子メールが加入者によって同一の人へ送信されるならばその人の権限が与えられたステータスを一時的ステータスから永久的ステータスまで格上げさせるというような、ＡＳＬマネージャによるさらなる分析のために用いられる。

【００２４】

図４Ａと図４Ｂには、標準的ＳＭＴＰ電子メール受信プロセス（従来技術）が、本発明に使用されている変更された電子メール受信プロセスと比較して示されている。図４Ａにあるように、標準的電子メール受信プロセスでは、電子メールは、インターネット上で送信者ソースからＳＭＴＰサーバによって受信され、サーバは、ユーザのインボックスにその電子メールを保管する。図４Ｂにあるように、本発明の変更された電子メール受信プロセスでは、受信された電子メールは、送信者のアドレスがＡＳＬリスト上の権限が与えられた人のものかどうか決定するため、リダイレクタ２０２による処理にかけられる。もし権限が与えられたものであったならば、ＳＭＴＰサーバは、ＳＭＴＰ受信マネージャ２０８がＡＳＬマネージャ２１１へ送信するためアドレス登録ステップ２１０の中で送信者のアドレスを電子メールにより得たのち、ユーザのインボックスにその電子メールを保管する。たとえ送信者がすでにＡＳＬ認可リスト上にあるとしても、受信された電子メールデータは、たとえば権限が与えられた人の電子メールが進行しながら受信されてユーザによって変更されないならばその人の権限が与えられたステータスを一時的ステータスから永久的ステータスまで格上げさせるというような、ＡＳＬマネージャによるさらなる分析のために用いられる。

【００２５】

プロセスのフローチャートである図５は、スパムプロセッサ２０３の働きを示している。リダイレクタ２０２の呼び出しルーチンからのリクエストであるブロック５０１では、電子メールが権限が与えられた送信者から来たものか否かに関係なく認証を求める。この要求は、電子メールがだれからのものかそしてだれへ送信されるのかというパラメータを識別する。スパムプロセッサ２０３は、ブロック５０２に示されているように、ＳＰＤＢデータベース２０３ａ内でユーザのＡＳＬリスト２０３ｂをルックアップするために送信先のアドレスを用いる。ルックアップ手順は、ユーザのＡＳＬリスト上にある次のＡＳＬ記録を読み、一致の有無を電子メール送信元アドレス（権限が与えられた人）から検査し、もし正しい記録の一致が無い場合には次の記録を読み、もし一致が見つかった場合にはブロック５０４に示されるようにテュリューバリュー（ＴＲＵＥ ＶＡＬＵＥ）が発行されることによって一致状態を実行し、さもなければ次の記録のために戻るというループ５０３に沿って進む。ブロック５０５では、もしテュリューバリューが発行されれば、ブロック５０５でフレンドに出力値を設定する働きが行なわれ、もし全リストが処理されたのちにテュリューバリューが発行されないならば、スパマーに出力値を設定する働きが行なわれる。ブロック５０６では、リターン値が呼び出しルーチン、つまりリダイレクタ２０２へのメッセージとして送信される。もしリターン値がスパマーであれば、標準的エラーメッセージが包含される。デフォルトオプションとして、もしユーザ用のＡＳＬが見つけられなければ、ＡＳＬリストがそのユーザのために作成されるまで一時的に電子メールの受信を可能にするためシステムはブロック５０７に示されるようにフレンド値へ戻る。要求処理ルーチンは、業界規格のＰＥＲＬプログラミングシンタックスを使用し、処理ルール

【００２６】
図６では、プロセスフローは、リダイレクタ２０２（図２参照）によって拒絶された電子メールを処理するためのウェブベースメッセンジャー（ＷＢＭ）のルーチンの詳細な働きを示している。別のウェブサイトアドレスで拒絶された送信者との相互対話を通してＷＢＭプロセスが実行される。図２のステップ２０４と対応し、フェーズ１でＷＢＭプロセスは、リダイレクタ２０２から送信されたとして電子メールを拒絶するためにバリューを返すＡＳＬルールによって、ブロック６０１において初期化される。ブロック６０２で、唯一のＩＤナンバーはＷＢＭデータベース内の電子メールに割り当てられ、４８時間というように一定の有効期限が決められる。ブロック６０３で、唯一のＩＤコードに沿ってスパマーの電子メール本文へリターンメッセージが追加され、彼らが加入者に接触し続けることを願う場合にＷＢＭウェブページへ行くことをスパマーに通知するよう送信者のメールアドレスへ返信される。そしてフェーズ２として示されるように、ＷＢＭは、スマパーがプロセスを完了するためＷＢＭサイトへ行くのを待つ。ブロック６０４で、スパマーはＷＢＭウェブサイトへアクセスし、用語のディスプレイされた諸条件と状態に同意する。ブロック６０５で、ＷＢＭプロセスは、スパマーに対応する電子メールへの応答時間の期限が切れなかったことを確認する。そしてＷＢＭは、応じているスパマーが機械的プログラムによって実行されていないことを保証するため、テスト処理に従う。例えば、ブロック６０６で、標準的でないフォントスタイルのワードがグラフィックイメージとして表示され、ブロック６０７でグラフィックの中に現れる単語をタイプすることをスパマーに促す。機械的プログラムは、識別されないフォントの単語のグラフィックイメージを読み取ることはできないであろう。

【００２７】
ブロック６０８で、もしＷＢＭプロセスが正しい単語が既にタイプされたと決定すれば、スパマーのステータスはユーザのＡＳＬリスト上のサスペクトへ格上げされる。ブロック６０９で、ＷＢＭプロセスは、サスペクトが加入者へ送信するべき短いメッセージを入力できるようなフォームを示す。たとえば、サスペクトは、スパム防止管理装置が電子メールを送信できるように更新されたことを確認することを加入者に求める。ブロック６１０で、「コンタクト」という単語をサブジェクト欄へ追加するというような、コードワードあるいはフラッグを包含するヘッダの変更に沿って、加入者のためのＡＳＭ電子メールボックスへ直接発送することにより電子メールとメッセージが送信される。コードワードは、権限が与えられた電子メールであると決定された他の電子メールと転送された電子メールを区別するため、図２にあるＡＳＭ電子メール登録ステップで識別される。次にブロック６１１で、今や加入者はサスペクトの電子メールを読むことができる。もし加入者がその電子メールへ応答を送信する場合、ＵＭＭ２１４を経て、サスペクトのステータスは自動的にフレンドへ格上げされるか、あるいは加入者はＩＳＰ電子メールサーバとの相互対話作用によりフレンドへステータスをマニュアルで格上げする。ブロック６１２で、もし電子メールがＷＢＭエラー応答オプションを欠いて拒絶されるべき誰かから来た電子メールであると加入者によって決定されるならば、加入者は任意に、ＵＭＭ２１４を経て、永久的にスパマーへステータスを格下げにする。

【００２８】
図７Ａのブロック図は、受信された電子メールを処理するための変更されたリダイレクタプロセスを示す図７Ｂと比較し、標準的ＳＭＴＰ送受信電子メール処理プロセス（従来技術）を示している。標準的プロセスでは、送信側ＳＭＴＰ７０１は、もし利用可能ならば接続に応じる受信側ＳＭＴＰ７０２への接続を要求する。そして送信側ＳＭＴＰは、受信者のメールアドレスへ送信するその送信電子メールループの中で作業を実行する。ブロック７０３で、送信側ＳＭＴＰは、受信者が存在するかあるいはそれがそのユーザのために電子メールを処理する権限を持っているかどうかを確認又は否定する。もし確認された場合には、送信側ＳＭＴＰはメッセージ本文を送信し、メッセージの終わりを示す。ブロック７０４で、受信側ＳＭＴＰは、メッセージ本文を受信し、それを受信者（あるいは一つ

ルボックスへ送信する。

【００２９】

図７Ｂで、送信側ＳＭＴＰ７０１と受信側ＳＭＴＰ７０２は、自らの平常の接続の設定を実行し、正当な受信者メールアドレスのための検査をする。しかしながら、当該スパムプロセッサ７０５と関連して実行される変更されたプロセスでは、送信者の送信元アドレスは、ブロック７０６に示されるように、後の利用のためにスパムプロセッサによって記憶される。ブロック７０７で、送信者の送信元アドレスと受信者の送信先アドレスは、以前に記述されたリダイレクタからの確認要請によってスパムプロセッサ７０５へ送信される。ブロック７０８で送信者が認可されているかどうかを決定するため受信者のＡＳＬリストを検査したのちに、スパムプロセッサは添付のエラーメッセージと共にフレンドの応答あるいはサパマーの応答へ戻る。もし応答がフレンドであるならば、電子メールが受信されうることを確認して出力が送信側ＳＭＴＰへ送られ、電子メールはいつもの通り受信側ＳＭＴＰへ送信される。ブロック７０９で、受信側ＳＭＴＰは電子メールを受信者のメールボックスに入れ、もし否定されたならば、送信者がフレンドの一人としてＡＳＬリスト上に認定されることを書き留めるメッセージを含むことができる。もし応答がスパマーであるならば、受信者が存在しないかあるいは受信側ＳＭＴＰは電子メールの受信を権限が与えられていないというエラーメッセージが送信側ＳＭＴＰへ戻される。もし（スパマーの確認されたステータスをもっていることと対照的に）スパムプロセッサからの応答によって送信者のステータスが知られていない送信者であると示された場合には、任意に、受信側ＳＭＴＰは、以前に述べたように（ブロック７１０に示されるように）ＷＢＭプロセスを経て電子メールを送信する。

【００３０】

図８で、略図は、以前に図２を参照し構成要素（ＡＳＬマネージャ）２１１として説明したＡＳＬマネージャの構造と働きを示している。ＡＳＬマネージャは、ＡＳＬルールプロセッサ８０３と相互対話し、スパムプロセッサデータベース（ＳＰＤＢ）203ａとデータを交換するＡＳＬオンデマンドプロセッサ８０１とＡＳＬスケジュラープロセッサ８０２とを有するように構成することが望ましい。ＳＭＴＰ送信マネージャ２１２へ送信され、そしてそこから受信された電子メールアドレスとＳＭＴＰ受信マネージャ２０８は、ＡＳＬルールプロセッサ８０３と関連して適切な規則を実行するＡＳＬオンデマンドプロセッサ８０１によって処理されるコンパーティブルなサード・パーティのプラグインを含む他の様々なソースからのコンテントを処理し、ＳＰＤＢ２０３ａに保存されたＡＳＬリストを作成し、ポピュレート（ｐｏｐｕｌａｔｅ）し、そして更新することもできる。例えば、コンテントは、電子メールクライアントと共に作業をしながらユーザアドレス入力を、関連ブラウザと共に作業しながらウェブサイトからのユーザアドレス入力を、Ｍｉｃｒｏｓｏｆｔ Ｏｕｔｌｏｏｋ（商標）Ａｄｄｒｅｓｓ Ｂｏｏｋのようなデスクトップコンタクトマネージャーへユーザが追加したアドレスを、あるいは他のコンタクトリストを、ユーザのクライアントプログラムと共に作業しながら第サード・パーティのソフトウェアによって生成された他のアドレス入力を好ましく処理するよう「ドラッグアンドドロップマネージャー」から受け取ることができる。

【００３１】

ＡＳＬスケジュラープロセッサ８０２は、さまざまな分析と維持機能のためにスケジュール通りタスクを実行するため使用される。これにより加入者のＡＳＬリスト、メールログ、そして他のデータファイルの、正確さと妥当性のために「権限が与えられた送信者」リストを絶えず改善することによって極めて豊富な調査が可能になる。例えば、プロセッサ機能は、加入者が送受信した電子メールのＡＳＬ電子メールログデータベース８０３ａを分析するためのＡＳＬ電子メールログアナライザ、加入者が頻繁に通信し合っている送信者の認可ステータスを格下げするかあるいは排除するための有効期限アナライザ、加入者が頻繁に通信し合っている送信者の認可ステータスを格上げするかあるいは永久的にマークするための高レベルアナライザ、さまざまな要素に基づいてフレンドあるいはスパマー

善するためサード・パーティのプラグインとプログラムによって生成されたデータを分析するための他のサード・パーティアナライザを含むことができる。

【００３２】

ＡＳＬルールプロセッサ８０３は、ＳＰＤＢデータベース２０３ａによって維持されたＡＳＬリストをどのように追加し、最新のものにし、変更するかを決定する（ＡＳＬマネージャールールデータベース内の）規則を包含する。ルールプロセッサは、スパムカプシステムを特徴づける改良し拡張するためにネットワークコミュニケーション業界の開発者の集団的パワーを利用したサード・パーティデータベース８０３ｂとアプリケーションプログラム８０３ｃを受け入れて共同利用するアーキテクチャーを持つことができる。このアーキテクチャーの究極の結果は、電子メールのダイナミックで知的な処理のために、スパム電子メールの総排除を超えてユーザにとって他のまたは将来必要になる極めて豊富で大変詳細なＡＳＬデータベースの構築を可能にする。

【００３３】

図９には、送信／受信電子メールとＡＳＬマネージャによって行なわれた働きの具体的な形態へのユーザコンタクトデータの処理例の詳細な実現例が示されている。基本的フローは、着信電子メールから得られた送信元アドレスを一致の判断のために比較するＡＳＬリスト（テーブルと呼ばれる）の各回線を通るループを構成するステップ９０１、一致した入力に対しどの状態またはステータスフラッグが設定されているかを決定し、テーブル上に維持される対応する状態規則を実行し、リターンバリューを戻すステップ９０２、そしてリターンバリューを基礎とし、コンディションテーブル上に示された対応する状態規則を実行し、この作用からの最終的リターンバリューとともに存続するステップ９０３から成る。このプロセスフローを経る一つの例に従うために、ステップ９０１は送信者アドレスｊｏｈｎ＠ｈｏｍｅ．ｃｏｍの送信元一致を見つけ、スッテプ９０２は「１２／１／２００３前の」有効期限状態を書きとめ、もし今日の日付が表示された有効期限以内であれば「ＴＲＵＥ」の値を戻すためにコンディションテーブル上の「以前」状態を実行し、ステップ９０３は（もし状態がＴＲＵＥであれば）送信者スタータス作用がフレンドであると書きとめ、（要素は不必要で）スパムプロセッサの正当応答としてフレンドの最終的リターンバリューを戻すためにアクションテーブル上の「フレンド」作用を実行する。

【００３４】

特別のプログラミングシンタックスあるいはＡＳＬマネージャルール処理の実行ロジックは、スパムプロセッサアプリケーションの開発者によると、どんな適当な方法にも変更することができる。いくつかのオプションの以下にある例は、使用されうる広範囲なアプローチを示している。

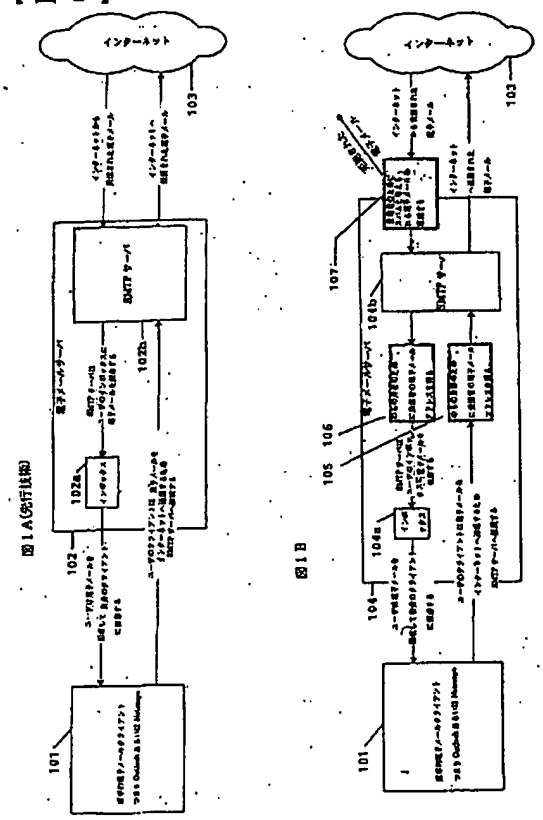
【００３５】

電子メールアドレスあるいはアドレスパターンを合わせること
（ａ）デフォルト：正確な一致
（ｂ）特別な電子メールアドレス：ｊｏｈｎ＠ｃｏｍｐａｎｙ．ｃｏｍ
（ｃ）ＵＮＩＸ標準的ワイルドカードマッチング
・ｍｉｃｒｏｓｏｆｔ．ｃｏｍ＝「Ｍｉｃｒｏｓｏｆｔ．ｃｏｍ」からのどれか
・ｍｉｃｒｏｓｏｆｔ＝その中でｍｉｃｒｏｓｏｆｔのどれか
・ｍｉｌ＝軍からのいずれかの電子メール
（ｄ）％ＢＬＡＣＫＨＯＬＥ％シンボルを使うことによる公知の「ブラックホールリスト」との一致
一致がＴＲＵＥである場合、実行するために条件とパラメータを使用する
条件がＴＲＵＥである場合、実行するために第二の作用とパラメータを使用する
加入者がこのアドレスへ電子メールを送信した最後の日付を使用する
加入者のアドレスに電子メールを送信した最後の日付を使用すること
記録が作成された日付を使用すること
使用できる条件の例

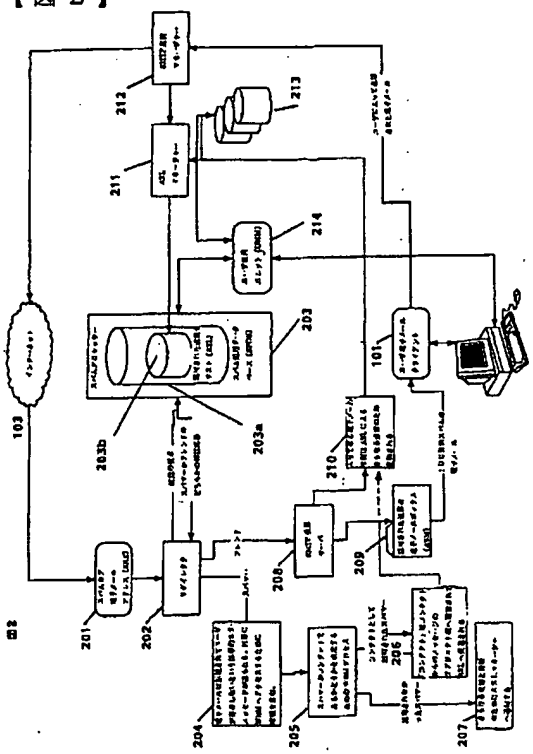
（ｂ）日付の範囲：４／１／２００４から５／２／２００４までに与えられたアドレスを使いなさい
（ｃ）特定の繰り返し時間：毎月の初週に他の時間、例えば、毎月の初週の間に受信可能なｎｅｗｓｌｅｔｔｅｒ@ｍａｇａｚｉｎｅ．ｃｏｍを除く
（ｄ）追加のユーザに定義された評価基準を考慮するように設計された外部のソフトウェアへのリンク；このことは第三者アプリケーションを考慮に入れておく。
【００３６】
所定の二次的行為によって呼び出されるメッセージの例
（ａ）標準的「エラー」
（ｂ）メッセージ本文の中に可変代替文があるカスタム。例えば
％ユーザ氏名％は送信者のメールアドレスで代入される
％スービッド（ｓｕｂｉｄ）％は加入者のＩＤコードである
％日付％は本日の日付である
（ｃ）「こんにちは、％ユーザ氏名％、スパムとして貴方は確認されました。ｈｔｔｐ：／ｗｗｗ．ｓｐａｍｋａｐｕ．ｃｏｍ／ｓｕｂｓｃｒｉｂｅｒ＝％ｓｕｂｉｄ％へ行き、もし貴方が本当に人であるならば私たちは貴方を迎えいれます。」
（ｄ）カスタムテキスト：「アメリカオンラインからの全電子メールアドレスを無条件で拒絶します。」
（ｅ）エラー応答内に所定のメッセージを送信する
（ｆ）電子メールとして所定の電子メールを送信する
（ｇ）ファイルを開き、その内容を電子メールで送信する
（ｈ）ファイルを開き、エラー応答としてその内容を送信する
（ｉ）送信者ステータスをスパマーあるいはフレンドへ設定する
（ｊ）短い期間（２４～４８時間）のあとで満期となるユニークのＩＤを作成する。このＩＤはサスペクトがＷＢＭへアクセスし、コンタクトになるために使用される。
（ｋ）ＳＭＴＰデフォルトエラーメッセージを与える
（ｌ）追加のユーザに定義された行為を考慮するように設計された外部ソフトウェアへリンクし、実行する。
【００３７】
【発明の効果】
要するに本発明は、着信電子メールの送信者アドレスを分析し、拒絶するべきか受信するべきかを権限が与えられた送信者の管理されたリストに従って決定するスパム電子メール拒絶方法を提供する。これは既に知られたスパマーのアドレスとして認められた送信者アドレスを持つ電子メールだけを取り除くことを試みて全電子メールを受信する現存のスパム防止処理システムからの重要な発展である。本発明方法は、権限が与えられていない電子メールを取り除くのではなく、むしろ認可されているものを除く全電子メールを拒絶するのである。システム内のＡＳＬマネージャは、「権限が与えられた送信者」リストを改善するために、発信及び着信電子メールのため送信者と受信者使用パターンを得て分析する。このデータの分析は、送信者アドレスがスパマーであると考えられるか否かの規則を基礎とした決定にとって堅固な基盤となる。このデータは、知られたスパマーのリストと対照的に、フレンドの「権限が与えられた送信者」リストを作成し、それによって頼んでもいない電子メールまたは求めていない電子メールが加入者の電子メールボックスへ達することが全くなくなるであろう。
【００３８】
本発明の指導原理の上記記述を考慮に入れると、他の多くの変更例と変形例を考えつくことができる理解される。以下の請求の範囲で定義されるように、かかる変更例及び変形例のすべては本発明の精神と範囲のように考えられる。
【図面の簡単な説明】
【図１】図１Ａは、本発明に係るシステムの概要を示す図１Ｂと比較したスパム送信者か

ステム（先行技術）を示すブロック図である。
【図２】図２は、本発明のスパム防止管理システムの最良の形態を説明するフローである。
【図３】図３Ａは、本発明に係る変更された電子メール送信プロセスを示す図３Ｂと比較した標準的ＳＭＴＰ電子メール送信プロセス（先行技術）を示すブロック図である。
【図４】図４Ａは、本発明に係る変更された電子メール受信プロセスを示す図４Ｂと比較した標準的ＳＭＴＰ電子メール受信プロセス（先行技術）を示すブロック図である。
【図５】図５は、本発明を実施するための最良の形態におけるルーチンを処理するスパム防止の働きを説明するフローである。
【図６】図６は、スパム防止管理方法によって最初に拒絶された電子メールを処理するためのウェブベースメッセンジャー（ＷＢＭ）のルーチンの詳細な処理を示すフローである。
【図７】図７Ａは、受信された電子メールを処理するための変更されたリダイレクタプロセスを示す図７Ｂと比較した標準的ＳＭＴＰ送受信電子メール処理プロセス（先行技術）を示すブロック図である。
【図８】図８は、スパム管理システム実施の最良の形態におけるＡＳＬマネージャの構造と働きを示す概要図である。
【図９】図９は、送信／受信電子メールの処理に関する実施例の詳細な実現と、ＡＳＬマネージャによって行なわれた働きの具体的な形態へのユーザコンタクトデータを示している。

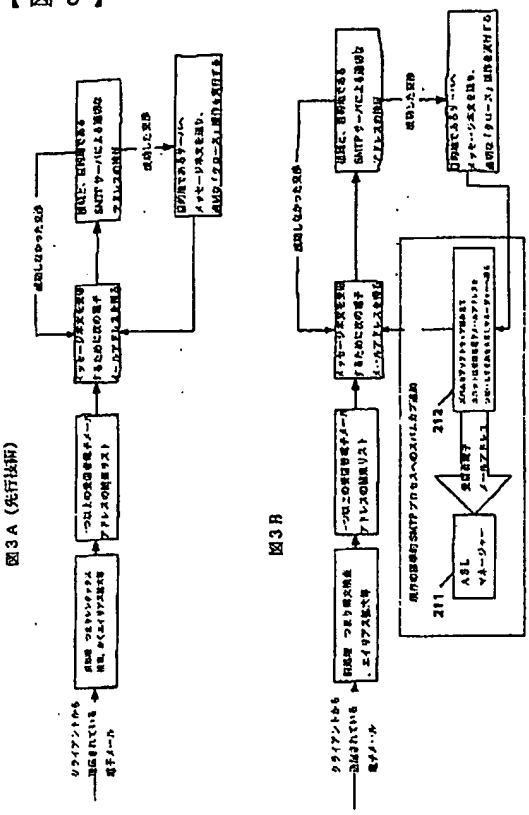
【図１】



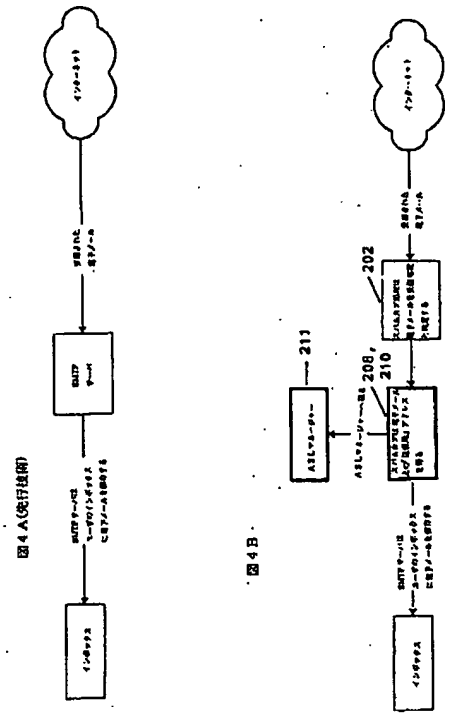
【図２】



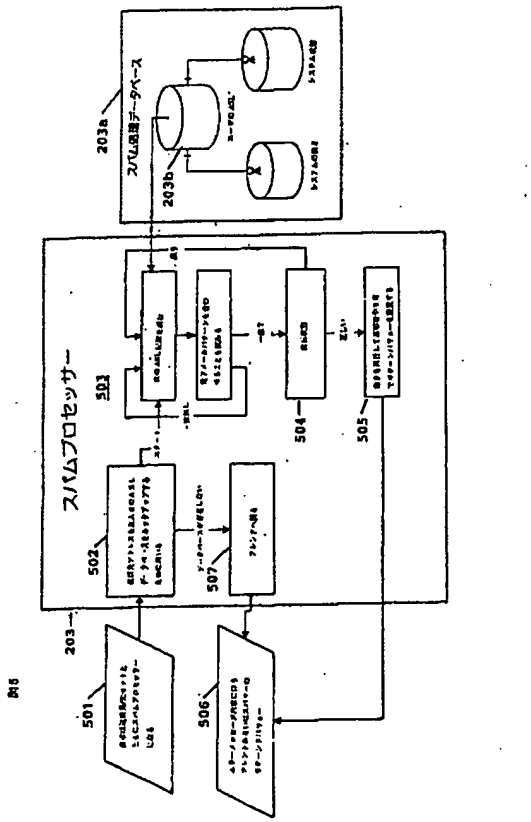
【図３】



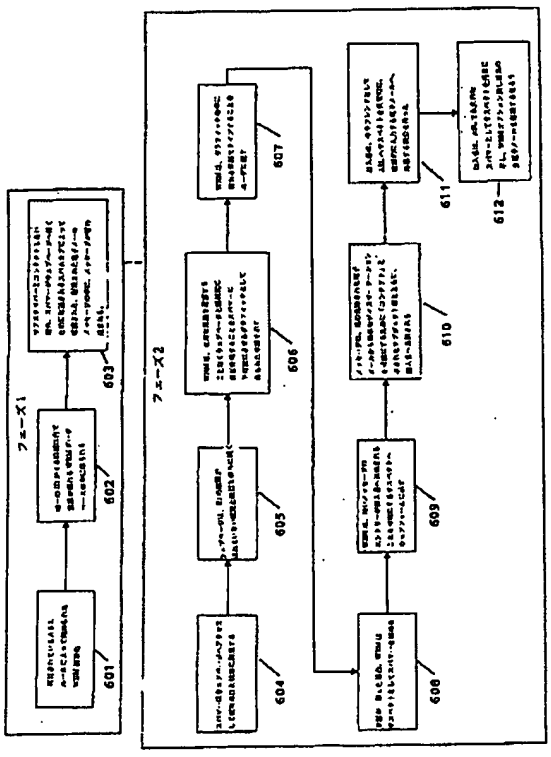
【図４】



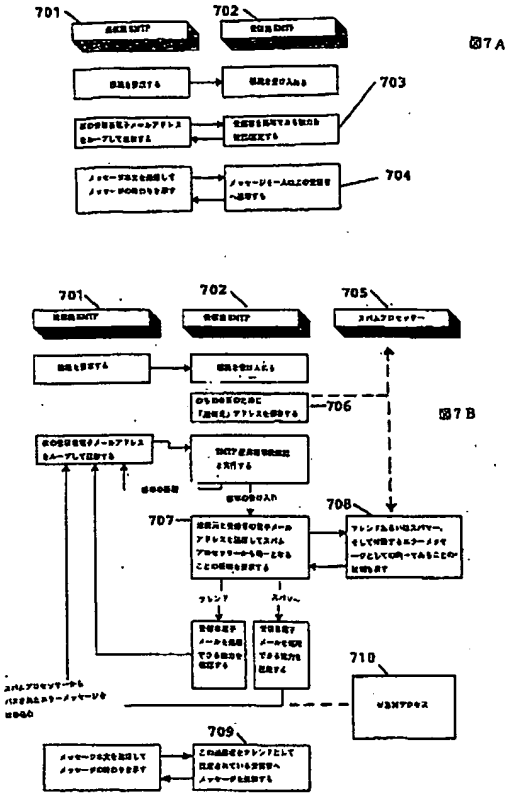
【図５】



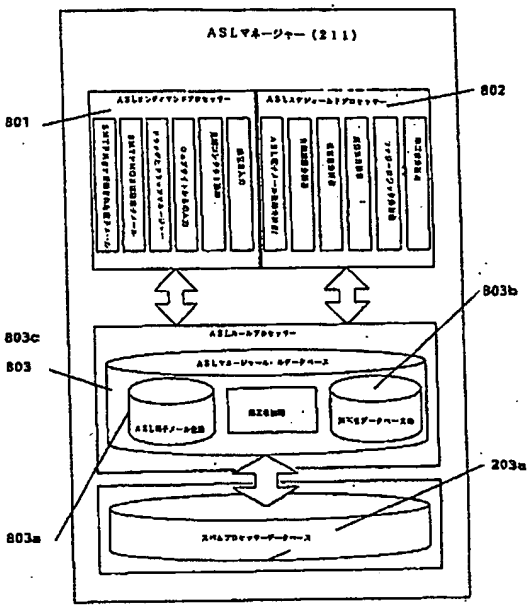
【図６】



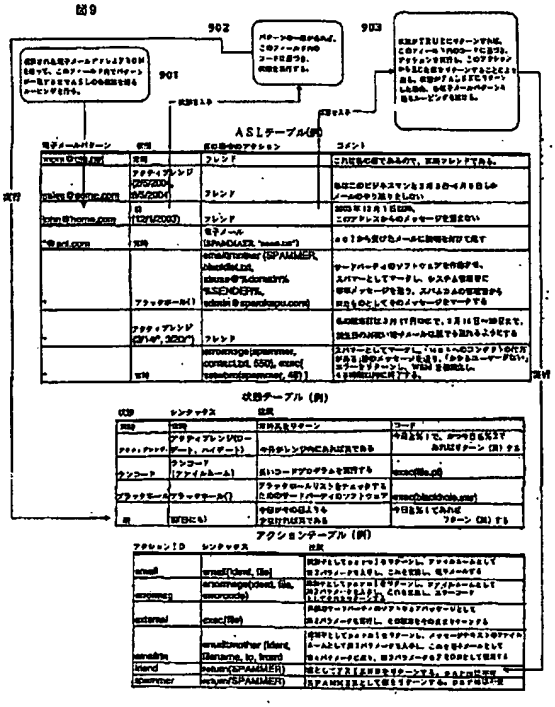
【図７】


701
702
703
704
705
706
707
708
709
710

【図８】


ASLマネージャー（211）
801
802
803
803a
803b
803c
203a

【図９】


901
902
903
ASLテーブル(例)
次段テーブル（例）
アクションテーブル（例）

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/16695 A1

(51) International Patent Classification⁷: G06F 7/00, 15/16, 17/00, H04N 1/00

(21) International Application Number: PCT/US00/23561

(22) International Filing Date: 25 August 2000 (25.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/150,025 1 September 1999 (01.09.1999) US
60/180,937 8 February 2000 (08.02.2000) US

(71) Applicant and
(72) Inventor: KATSIKAS, Peter, L. [US/US]; Suite 245, 2800 Woodlawn Drive, Honolulu, HI 96822 (US).

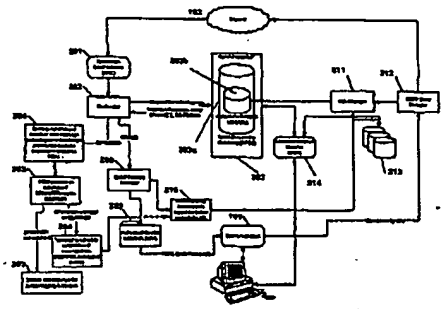
(74) Agent: CHONG, Leighton, K.; Ostrager Chong & Flaherty, Suite 1200, 841 Bishop Street, Honolulu, HI 96813 (US).

(81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM FOR ELIMINATING UNAUTHORIZED ELECTRONIC MAIL



(57) Abstract: A system for eliminating unauthorized email sent to a user on a network employs an email-receiving server (104) connected between the network and the user's email client (101) for receiving email addressed to the user and rejecting those in which the sender address does not match any of sender addresses maintained on an "authorized senders" list (ASL list). The ASL lists are maintained by an ASL manager (211) in an ASL database (203a) operable with a spam processor module (203). A redirector module (202) rejects the email if, upon sending a request for validation to the spam processor module, the sender's address does not match any authorized sender address on the ASL list. Email rejected by the redirector module is redirected to a web-based messaging (WBM) module (204, 205) which sends a message to the sender to confirm that the sender is a legitimate sender of email to the intended recipient. If the sender logs on to confirm their status, the WBM module executes an interaction procedure which can only be performed by a human, in order to ensure that the confirmation procedure is not performed by a mechanical program. The ASL manager maintains the ASL lists based upon sender address data collected from various sources an analyses of various email usage factors, including sent email, received email, contact lists maintained by the user, user preference inputs, third party programs, etc.

WO 01/16695 A1

WO 01/16695 A1

SYSTEM FOR ELIMINATING UNAUTHORIZED ELECTRONIC MAIL

FIELD OF THE INVENTION

This invention relates to a system for eliminating unwanted email, and particularly to one in which all email must be recognized as sent by an authorized sender in order to be accepted.

BACKGROUND OF THE INVENTION

Unwanted or unauthorized email is a significant bane for users on worldwide networks, such as the current public Internet. Once a person's email address becomes known in a network system, it can easily be replicated in computerized lists and passed on electronically to an unlimited number of parties who have not been authorized or invited to send email to the user. A user's electronic mailbox can become inundated with such unauthorized email. Unauthorized or unwanted email is referred to generically in the industry by the term "spam", although the term is not intended to be associated with or to disparage the popular canned meat product sold under the trademark "Spam" by Hormel Corp. The user may have an email address with a commercial information service provider (ISP) service which limits the amount of email that can be accepted and/or stored or which charges the user by the volume received. The user may also waste a significant amount of time opening and reviewing such unwanted email. Unauthorized email may also be sent by unscrupulous persons who may enclose a virus or noxious software agent in the email which can infect the user's computer system, or which can be used as an unauthorized point of entry into a local network system that handles the user's email.

Most, if not all, of the current software to control the receipt of spam is based upon the use of identifying lists of known spam sources or senders ("spammers"). Such conventional spam control software functions on the basis of receiving all email as authorized unless a sender is identified as being on the exclusion list and the email can be filtered out. This approach is only as good as the identifying list and cannot guarantee that the user will not receive spam. Spammer lists require frequent updating and must be distributed in a timely manner to all subscribers to the spam control software or service. Sophisticated spammers frequently change their source Internet address, and can defeat attempts to keep exclusion lists current. They can also route the unwanted email through the Internet servers of other parties so as to disguise the source of the emails through innocuous or popularly recognized names. A user's email address may also become known to large numbers of individuals in public chat rooms or on public bulletin boards. Unwanted email sent by individuals are not tracked on spammer lists, because the sending of email by individuals is technically not spamming.

SUMMARY OF THE INVENTION

Accordingly, it is a principal object of the present invention to provide a spam control system that cannot be defeated by spammers who frequently change their source addresses or disguise themselves by routing email through other servers, or by individuals who send email that are not invited or authorized by the user. It is a particular object of the invention that the system of the invention reject all email as unauthorized unless the sender is recognized as being on the user's acceptance list.

In accordance with the present invention, a system for eliminating unauthorized email sent to a user on a network comprises:

(a) an email client for allowing the user to receive email sent on the network addressed to a unique email address of the user,

(b) an email-receiving server connected between the network and the email client for receiving email addressed to the unique email address of the user, said email-receiving server having an authorized senders list (ASL) module which maintains an ASL list of email addresses of external users authorized to send email to the user, and

(c) an email rejection module operable with the ASL module for rejecting the receipt of email sent to the email address of the user if the email address of the sender is not one that is maintained on the ASL list for the user.

In a preferred embodiment, the system's ASL module includes an ASL database for storing ASL lists of authorized sender addresses for respective subscribers of the system, a spam processor module for checking the ASL lists for matches, and an ASL manager for creating, maintaining, and updating the ASL lists. A redirector module rejects email if, upon sending a request for validation to the spam processor module, the sender's address does not match any authorized sender address found on the ASL list. Email rejected by the redirector module is redirected to a web-based messaging (WBM) module which sends a message notifying the sender to confirm that the sender is a legitimate sender of email to the intended recipient. If the sender logs on to confirm their status, the WBM module executes an interaction procedure which can only be performed by a human, in order to ensure that the confirmation procedure is not performed by a mechanical program. The ASL manager maintains the ASL lists based upon sender address data collected from various sources and analyses of various email usage factors, including sent email, received email, contact lists maintained by the user, user preference inputs, third party programs,etc.

The invention also encompasses associated methods of performing the above functions, as well as related software components which enable these functions to be performed.

Other objects, features, and advantages of the present invention will be described in further detail below, with reference to the following drawings:

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1A is a block diagram illustrating a standard Internet email system using the conventional method for filtering email from spammers (Prior Art), as compared to FIG. 1B which shows a conceptual overview of a system in accordance with the present invention.

FIG. 2 is a process flow diagram for a preferred embodiment of the anti-spam system of the present invention.

FIG. 3A is a block diagram illustrating a standard SMTP send email process (Prior Art), as compared to FIG. 3B which shows a modified send email process used in the present invention.

FIG. 4A is a block diagram illustrating a standard SMTP receive email process (Prior Art), as compared to FIG. 4B which shows a modified receive email process used in the present invention.

FIG. 5 is a process flow diagram illustrating the operation of an anti-spam processing routine in the preferred embodiment of the invention.

FIG. 6 is a process flow diagram illustrating the detailed operation of a Web-Based Messenger (WBM) routine for handling email initially rejected by the anti-spam control.

FIG. 7A is a block diagram illustrating a standard SMTP send-receive email handling process (Prior Art), as compared to FIG. 7B which shows a modified Redirector process for handling received email.

FIG. 8 is a schematic diagram illustrating the structure and operation of the ASL Manager in the preferred embodiment of the spam control system.

FIG. 9 illustrates a detailed implementation of examples of processing of email send/receive and user contact data into specific forms of actions taken by the ASL Manager.

DETAILED DESCRIPTION OF INVENTION

In contrast to the known approaches of existing spam control methods of accepting all email unless listed on an exclusion list as unauthorized, the fundamental principle of the present

invention is to reject all email unless listed on an inclusion list as authorized. In this manner, it is possible to filter out email that comes from unrecognized spammers as well as individuals who send email that is uninvited by the user. Unlike the known email filtering systems, the present invention does not attempt to filter out the unwanted email after it has been accepted. Rather, it outright rejects the email at the earliest entry level. Thus, the invention operates on the premise that all email will be treated as unauthorized unless the sender is found to be on an "authorized senders" list in order to be accepted by the user. This provides an inherently powerful and 100% effective spam control solution in an environment where spammers can instantaneously change their source address or apparent identity and individuals in public areas can obtain email addresses of other users and send them unwanted email.

The following is a detailed description of one preferred embodiment of a system for implementing the invention concept. In this embodiment, the spam control system intelligently formulates the "authorized senders" list based upon an ongoing analysis of the user's email usage, such as to whom and with what frequency sent email is addressed to other users, and through the gathering of high-level user contact data, such as a user's known contacts and associates identified on other lists or files maintained by the user which indicate persons considered as authorized. The "authorized senders" list may also be updated and manipulated by the user at any time to add or remove authorized senders. While this specific implementation is used, and certain components are provided and configured to be interoperable in the described ways, it is to be understood that the full scope of the invention is deemed to encompass many other suitable modifications and variations to the described guiding principles of the invention.

FIG. 1A is a block diagram of a standard email system for sending and receiving email on the Internet and is used to explain the conventional method for filtering out email from spammers. The system follows a standard industry protocol for handling email on the Internet, referred to as SMTP. Users typically subscribe with a chosen ISP for Internet access and related services, including email services. The users access the Internet through the ISP using a dialup or high-speed line connection and a standard browser. The browser includes or functions with a standard email client 101, such as the Outlook ™ email client distributed by Microsoft Corp., headquartered in Bellevue, Washington, or the Netscape ™ email client used by AOL/Netscape, headquartered in Fairfax, Virginia. The ISP operates at a website address corresponding to its domain name which is addressable by users on the Internet. The ISP's service functions are performed for a large number of subscribers through one or more servers. Typically, an email server 102 is used to handle the email service functions. Email sent to the ISP from the Internet is received at SMTP Server 102b, where various administrative functions are performed, such as checking whether the addressee is an authorized subscriber of the ISP, then the email is placed in a storage space reserved for that user, referred to as Inbox 102a. When users connect to the ISP, they can retrieve their email and store it with their own email client (on their own computer). Users can send email by composing it locally at their email client, then uploading it to the SMTP Server 102b at the ISP, which then routes it to the recipient's email address on the Internet.

Conventional anti-spam control can be implemented with the SMTP Server and/or at the email client. Many ISPs implement an exclusion list of known spammers at the SMTP Server. In addition, they commonly allow a user to filter out unwanted email from certain senders known to the user. For example, the user's email client may have a filtering function that allows the user to input unwanted sender email addresses to the SMTP Server so that email received by the SMTP Server can be filtered out before being put into the user's inbox. Further, independent software vendors sell sophisticated email handling programs that work with the user's email client. For example, some handling program have functions for categorizing received email into topical file folders, and email from unrecognized senders may be put into a "Miscellaneous" or "Unrecognized" file folder.

In FIG. 1B, a conceptual overview of a system in accordance with the present invention is shown. As before, the standard email client 101 is connected to an email server 104 for sending and receiving email to and from the Internet via SMTP Server 104b and Inbox 104a. However, in this modified email server 104, an Authorized Sender List (ASL) Manager captures recipient email addresses from email sent by the user, as shown at block 105, and also captures sender email addresses from email sent to the user, as shown at block 106. The ASL Manager analyzes the captured sender email addresses and recipient email addresses and employs certain pre-defined rules (described in further detail below) to add or remove email addresses from the "authorized senders" list, referred to as the ASL List or Database. The ASL List is used by the SMTP Server 104b to accept only email from senders on the ASL List and place the accepted email in the user's Inbox 104a, while rejecting all other email as "unauthorized", as indicated at block 107.

Referring to FIG. 2, the process flow for the operational steps of the anti-spam system of the present invention will now be described. Certain terms used in the description are defined below:

SPAMKAPU: An example of the spam control system of the invention.

SUBSCRIBER: A person subscribing to an ISP email service that is using the spam control system of the invention.

FRIEND: An email-sending source that is authorized by the spam control system to send email to the SUBSCRIBER.

SPAMMER: An email-sending source that is not authorized to send email to the SUBSCRIBER, which is commonly understood to be an unknown or unauthorized party that is using a manual or computerized email list mailing program to send large volumes of emails repetitively through the Internet.

CONTACT: An email-sending source that has been identified by the system as a legitimate correspondent of the SUBSCRIBER is authorized by the system to send email to the SUBSCRIBER.

SUSPECT: An email sending source that has not yet been identified as either a SPAMMER or a CONTACT.

Email sent from the Internet (103) is sent to the email address of the ISP for the SUBSCRIBER, referred to in block 201 as the SpamKapu Email Address (SKE). Received email must first pass through the Redirector 202. The Redirector 202 sends a request for validation for the email from the Spam Processor 203 which maintains the Spam Processing Database (SPDB) 203a, including the Authorized Senders List (ASL) 203b. The SPDB Database and ASL List are the heart of SPAMKAPU, as they contain the lists of persons authorized to send email to the respective SUBSCRIBERS of the system. The Spam Processor 203 sends a response, either that the sender's address on the email is not authorized on the ASL List, i.e., is a SPAMMER, or is authorized on the ASL List, i.e., is a FRIEND. If the response is that it is a SPAMMER, the Redirector 202 rejects the email, as shown at block 204, such as by sending a standard error message to the sending server that the user as addressed does not exist.

As a refinement to the system, a Web-Based Messenger (WBM) process at block 205 may be set up to provide a corrective procedure in the event that the rejected email is from someone not authorized but not listed permanently on the ASL List as a SPAMMER. The unauthorized email may actually be from a person who has not been previously processed in the anti-spam system but who has a legitimate reason to reach the SUBSCRIBER. The WBM process 205 is set up as part of the spam control system to which the rejected email is redirected. Upon receipt of the redirected email, the WBM process stores it in the WBM database, assigning the email a unique ID code and also an expiration date. The WBM process then sends an error response email to the email sender, who is now treated as a SUSPECT. For example, the error message may read:

> "An email sent by you to SUBSCRIBER's address was redirected to this site as being sent from an unrecognized sender address which may be a source of spam email. If you would like to confirm yourself as a person with legitimate reason to reach the SUBSCRIBER, please visit the WBM site (or send a reply email) and confirm your status as a CONTACT."

The WBM may have a separate web site address for interactions with SUSPECTS, or it may be set up to receive and recognize email responses from SUSPECTS. When a SUSPECT receives the error response email, if they are a legitimate CONTACT for the SUBSCRIBER, they may elect to go to the WBM site or send a reply email in order to confirm their status as a legitimate CONTACT. If done before the expiration date, the WBM process will add a special codeword such as "contact:" to the subject line of the redirected email, as shown at block 206, and re-route the email to the Authorized Sender Mailbox (ASM) 209. The sender address for email re-directed through this process is also stored (as indicated by the dashed line to block 210) and logged for further analysis by the ASL Manager 211, to determine if the status of the SUSPECT should be upgraded to FRIEND and added to the ASL 203b. If the SUSPECT does not respond, this fact is also sent to the ASL Manager for further analysis. The extra confirmation step effectively eliminates SPAMMERS since they use automated programs to send out

batch email and typically will not take human response time to log on to the WBM site or send a reply email to confirm their legitimate status.

If the Spam Processor sends a validation response that the sender is a FRIEND, then the Redirector 202 passes the email to the SMTP Receive Manager, at block 208, which performs its administrative function of checking the SUBSCRIBER's status and storing the email in ASM 209, which is the SUBSCRIBER'S Inbox. The user can now collect their email from the ASM Inbox (using standard Internet protocols such as POP3 or IMAP4) through the user email client 101 on their computer. Their email is 100% spam-free, since all email from senders not recognized by the system as authorized has been rejected. The SMTP Receive Manager 208 is also configured to log the information of receipt of the email from a FRIEND and send it to the ASL 203b for further analysis, as indicated at block 210.

Users send email composed on and sent from the email client 101 via standard SMTP protocols to the ISP's email server. The ISP's SMTP server is responsible for providing users with email addresses within the system, and sending users' email to the recipients' email addresses on the Internet 103. In the SPAMKAPU invention system, an SMTP Send Manager 212 is provided to intervene in the usual send email process. The SMTP Send Manager 212 copies header information from all outgoing email and sends the data to the ASL Manager 211, then sends the email on to its intended destination. The ASL Manager 211 performs one of the key functions in the invention system. It analyzes the header data from sent email and data from other data sources 213 maintained by the ISP email server system, such as email logs and user-supplied lists. On the basis of its analysis routines (to be described in further detail below), the ASL Manager 211 checks, populates, and updates the SPDB Database and ASL List with the email addresses and other data on senders authorized to send email to the SUBSCRIBERS. The SPAMKAPU system also includes User Maintenance Modules (UMM) 214 which allows the user to interact with and upload user information to SPAMKAPU for further customization of SPAMKAPU's email operations for the user.

Referring to FIGS. 3A and 3B, a standard SMTP send email process (Prior Art) is shown compared to a modified send email process used in the present invention. In the standard send email process, in FIG. 3A, email sent from the user's email client to the ISP's email server may be pre-processed, such as checking for correct syntax, alias expansion, etc., and to identify the list of recipient email addresses (could be 1 or more). The server email manager gets each recipient email address in turn and attempts to establish a connection to the destination SMTP server and verify if the recipient email address is proper. If negotiation is unsuccessful, an error message is returned to the sending SMTP server. If negotiation is successful, the sending server sends the message body to the destination server and performs a proper "close connection" operation. In the modified send email process of the invention, in FIG. 3B, the email sent from the client is pre-processed, recipient(s) are identified, and connection(s) with the destination server(s) are attempted as usual. Upon successful negotiation, the SPAMKAPU SMTP Send Manager 212 copies the successful recipient email address(es) and sends the

data to the ASL Manager 211. On the assumption that the SUBSCRIBER authorizes email to be received from any person the SUBSCRIBER has sent email to, the proper email addresses of persons to whom the SUBSCRIBER has sent email are added to the ASL List of persons authorized to send email to the SUBSCRIBER. The sent email data can be used in further analyses by the ASL Manager, e.g., to upgrade a person's authorized status from temporary to permanent if more than a threshold number of email is sent by the SUBSCRIBER to the same person.

Referring to FIGS. 4A and 4B, a standard SMTP receive email process (Prior Art) is shown compared to a modified receive email process used in the present invention. In the standard receive email process, in FIG. 4A, email is received by the SMTP server from sender sources on the Internet and the server stores the email in the user's Inbox. In the modified receive email process of the invention, in FIG. 4B, the received email is subjected to processing by the Redirector 202 to determine if the sender's address is that of an authorized person on the ASL List. If authorized, the SMTP server stores the email in the user's Inbox after the SMTP Receive Manager 208 captures the sender's address on the email in the address log step 210 to be sent to the ASL Manager 211. Even though the sender is already on the ASL authorized persons list, the received email data can be used in further analyses by the ASL Manager, e.g., to upgrade a persons authorized status from temporary to permanent if email from that person is received on an ongoing basis and has not been changed by the user.

In FIG. 5, a process flow diagram illustrates the operation of the Spam Processor 203. At block 501, a request from the calling routine, here Redirector 202, seeks validation whether a received email is from an authorized sender. The request identifies the parameters who the email is FROM and who it is sent TO. The Spam Processor 203 uses the TO address to lookup that user's ASL list 203b in the SPDB Database 203a, as indicated at block 502. The lookup procedure follows a loop 503 of reading the next ASL record on the user's ASL list, checking for a match to the email FROM address (authorized person), reading the next record if there is no match of the current record, executing the match condition by issuing a TRUE value if found, otherwise returning for the next record, as indicated at block 504. At block 505, if a TRUE VALUE is issued, then at block 505 the action is taken of setting the output value to FRIEND, otherwise if no TRUE value is issued after the entire list has been processed, the action is taken of setting the output value to SPAMMER. At block 506, the returned value is sent as a message to the calling routine, i.e., the Redirector 202. If the returned value is SPAMMER, a standard error message is included. As a default option, if no ASL list is found for the user, the system returns the value FRIEND, as indicated at block 507, in order to allow the email to be accepted as a temporary condition until an ASL list can be established for that user. The request processing routine can be implemented using industry standard PERL programming syntax and incorporating a PERL interpreter to execute the processing rules.

In FIG. 6, a process flow diagram illustrates the detailed operation of the Web-Based Messenger (WBM) routine for handling email rejected by the Redirector 202 (see FIG. 2). Preferably, the

WBM process is implemented via interaction with a rejected sender at a separate Web site address. In Phase 1, corresponding to step 204 in FIG. 2, the WBM process is initialized at block 601 by the ASL rule returning a value for rejecting an email as sent from a SPAMMER by the Redirector 202. At block 602, a unique ID number is assigned to the email in the WBM database and a given expiration date is set, e.g., 48 hours. At block 603, a return message is added along with the unique ID code to the body of the SPAMMER's email and sent back to the sender's email address in order to notify the SPAMMER to go to the WBM web page if they wish to follow through with contacting the SUBSCRIBER. The WBM then waits for the SPAMMER to go to the WBM site to complete the process, referred to as Phase 2. At block 604, the SPAMMER accesses the WBM web site and agrees to the displayed terms and conditions of usage. At block 605, the WBM process verifies that the time for response for the email corresponding to the ID number has not expired. The WBM then follows a test procedure to ensure that the responding SPAMMER is not being implemented by a mechanical program. For example, at block 606, a word stylized in non-standard font can be displayed as a graphic image, and at block 607 the SPAMMER is prompted to type the word that appears in the graphic. A mechanical program would not be able to read a graphic image of a word in unrecognizable font. At block 608, if the WBM process determines that a correct word has been typed, the SPAMMER's status is upgraded to SUSPECT on the user's ASL list. At block 609, the WBM process presents a form to enable the SUSPECT to enter a short message to be sent to the SUBSCRIBER. For example, the SUSPECT can ask the SUBSCRIBER to make sure the anti-spam control has been updated to allow email. At block 610, the email and message is sent, by routing directly to the ASM email box for the SUBSCRIBER, along with modification of the header to include a codeword or tag, e.g., adding the word "contact:" to the subject line. The codeword can be discerned in the ASM email logging step 210 in FIG. 2, in order to differentiate the redirected email from other email determined to be authorized email. At block 611, the SUBSCRIBER can now read the SUSPECT's email. If the SUBSCRIBER sends a reply to the email, the SUSPECT's status may be automatically upgraded to FRIEND, or the SUBSCRIBER may upgrade the status to FRIEND manually by interaction with the ISP email server through the UMM 214. At block 612, if the SUBSCRIBER determines that the email is from someone whose email should be rejected without a WBM error reply option, the SUBSCRIBER may optionally downgrade the status permanently to SPAMMER through the UMM 214.

Referring to FIG. 7A, a block diagram illustrates a standard SMTP send-receive email handling process (Prior Art), as compared to FIG. 7B which shows a modified Redirector process for handling received email. In the standard process, the Sender-SMTP 701 requests connection to the Receiver-SMTP 702, which accepts the connection if available. The Sender SMTP then performs the task in its Send Email loop of sending the recipient's email address. At block 703, the Receiver-SMTP confirms or denies whether the recipient exists or whether it has authority to process email for this user. If confirmed, the Sender-SMTP sends the message body and marks the end of the message. At block 704, the Receiver-SMTP receives the message body and sends it to the email box of the recipient (or recipients if the message is sent to more than one recipient at that SMTP server address.

In FIG. 7B, the Sender-SMTP 701 and Receiver-SMTP 702 perform their usual establishing of a connection and check for valid recipient e-mail address. However, in this modified process implemented in conjunction with the Spam Processor 705, the sender's FROM address is stored by the Spam Processor for later use, as indicated at block 706. At block 707, the sender's FROM address and the recipient's TO address are sent to the Spam Processor 705, by a request for validation by the Redirector as described previously. At block 708, after checking the recipient's ASL list to determine whether the sender is authorized, the Spam Processor can return a response of FRIEND or a response of SPAMMER with an accompanying error message. If the response is FRIEND, an output is sent to the Sender-SMTP confirming that the email can be received, and the email is sent to the Receiver-SMTP as usual. At block 709, the Receiver-SMTP puts the email in the recipient's email box and, if desired, can include a message noting that the sender was identified on the ASL list as a friend. If the response is SPAMMER, then an error message is returned to the Sender-SMTP that the recipient does not exist or the Recipient-SMTP is not authorized to accept the email. Optionally, the Receiver-SMTP may send the email through the WBM process, as described previously (indicated at block 710), if the response from the Spam Processor indicates that the status of the sender is an unknown sender (as opposed to having the confirmed status of SPAMMER).

In FIG. 8, a schematic diagram illustrates the structure and operation of the ASL Manager, previously described as component 211 with respect to FIG. 2. The ASL Manager preferably is structured to have an ASL On-Demand Processor 801 and an ASL Scheduler Processor 802, both of which interact with an ASL Rules Processor 803, which also exchanges data with the Spam Processor Database (SPDB) 203a. Email addresses sent to and received from the SMTP Send Manager 212 and SMTP Receive Manager 208 are processed by the ASL On-Demand Processor 801 which executes the appropriate rules in conjunction with the ASL Rules Processor 803. Content from a variety of other sources, including compatible third party plug-ins, can also be processed to create, populate, and update the ASL Lists stored in the SPDB 203a. For example, content may be received from a "Drag and Drop Manager" for conveniently handling user address inputs while working with the email client, user address inputs from Web sites while working with an associated browser, addresses added by the user to a desktop contact manager, such as the Microsoft Outlook ™ Address Book, or other contact lists, and other address inputs generated by third party software that can operate with the user's client programs.

The ASL Scheduler Processor 802 is used to process tasks on a scheduled basis for various analysis and maintenance functions. This allows a very rich examination of the SUBSCRIBER's ASL list, mail log, and other data files, to continually refine the "authorized senders" list for accuracy and relevance. For example, the processor functions can include: an ASL Mail Log Analyzer for analyzing the ASL Mail Log database 803a of the SUBSCRIBER's received and sent emails; an Expiration Date Analyzer for setting and enforcing expiration dates for authorized senders to be re-authorized; a Low Volume Analyzer for downgrading or eliminating the authorization status of senders with whom the

SUBSCRIBER communicates very infrequently; a High Volume Analyzer for upgrading or permanently marking the authorization status of senders with whom the SUBSCRIBER communicates very frequently; a Fuzzy Logic Analyzer for making qualitative decisions as to FRIEND or SPAMMER status based on a variety of factors; and other Third Party Analyzers for analyzing data generated by third party plug-ins and programs to refine the ASL list.

The ASL Rules Processor 803 contains the rules (in an ASL Manager Rules Database) that determine how to add, update or modify the ASL Lists maintained in the SPDB Database 203a. The Rules Processor can have an architecture that readily accepts and interoperates with third party databases 803b and applications programs 803c in order to harness the collective power of developers in the network communications industry to continually improve and extend the SPAMKAPU system's feature set. The ultimate result of this architecture is to enable the creation of a very richly detailed ASL database which goes beyond even the total elimination of spam email into other or future needs of users for the dynamic and intelligent handling of email.

In FIG. 9, a detailed implementation is illustrated of examples of processing of email send/receive and user contact data into specific forms of actions taken by the ASL Manager. The basic process flow consists of: Step 901 of looping through each line of an ASL list (called a Table) comparing the FROM address captured from an incoming email for a match; Step 902 of determining whatever condition or status flag has been set for the matched entry, then executing the corresponding condition rule as maintained on the Condition Table, resulting in return of a Return Value; and Step 903, based on the Return Value, executing the corresponding action rule as maintained on the Action Table, and ending with a Final Return Value from this action. To follow one example through this process flow, Step 901 finds a FROM match of the sender address john@home.com, Step 902 notes the expiration date condition "before 12/1/2003" and executes the "before" condition on the Condition Table to return a value of "True" if today's date is less than the indicated expiration date, and Step 903 notes that the sender status action (if condition is True) is "friend" and executes the "friend" action on the Action Table to return a Final Return Value of FRIEND (no parameters needed) as the validation response of the Spam Processor.

The specific programming syntax or execution logic of the ASL Manager rules processing may be varied in any suitable manner depending on the developer of the Spam Processor application. The following examples of some options for ASL Manager actions illustrate a wide range of approaches that may be used:

MATCHING AN EMAIL ADDRESS OR ADDRESS PATTERN:
(a) Default: exact match
(b) A specific email address: john@company.com
(c) UNIX Standard wildcard matching:
*.microsoft.com = anything from "Microsoft.com"
"microsoft" = anything with microsoft in it
*.mil = any email from the military
(d) Matching any known "blackhole list" by using a %BLACKHOLE% symbol.

USING A CONDITIONAL AND PARAMETERS TO EXECUTE IF THE MATCH IS TRUE

USING A SECONDARY ACTION AND PARAMETERS TO PERFORM IF THE CONDITIONAL IS TRUE.

USING THE LAST DATE THE SUBSCRIBER SENT EMAIL TO THIS ADDRESS

USING THE LAST DATE THIS ADDRESS SENT EMAIL TO THE SUBSCRIBER

USING DATE THE RECORD WAS CREATED

EXAMPLES OF CONDITIONALS THAT CAN BE USED:
(a) Expiration dates: use a given address until 2/12/2004
(b) Date ranges: use a given address from 4/1/2004 to 5/2/2004
(c) Specific recurring times: first week of every month but no other time, e.g., newsletter@magazine.com acceptable during 1st week of each month.
(d) A link to external software designed to allow for additional user-defined criteria; this allows for third party applications

EXAMPLES OF MESSAGES THAT MAY BE INVOKED BY A GIVEN SECONDARY ACTION
(a) Standard "error"
(b) Custom with variable substitution in the message body, e.g.:
%username% is substituted with the sender's email address
%subid% is the ID code of the subscriber
%date% is today's date
(c) "hello %username% you have been identified as spam, go to http://www.spamkapu.com/subscriber=%subid% and if you're really human we'll let you in.
(d) Custom text: "All email addresses from America Online are unconditionally rejected"
(e) Send a given message in the error response.
(f) Send a given message as an email.
(g) Open a file and email its contents
(h) Open a file and send its contents as an error reponse.
(i) Set the sender's status to SPAMMER or FRIEND
(j) Create a unique ID that will expire after a short time period (24-48hrs). This id can be used by the SUSPECT to access the WBM and become a CONTACT.
(k) Give SMTP default error message
(l) Link and execute external software designed to allow for additional user-defined actions; this allows for third party applications.

In summary, the present invention provides a spam email rejection method which analyzes the sender address of incoming email and determines whether it is to be rejected or accepted depending upon managed lists of authorized senders. This is a significant departure from existing anti-spam processing systems which accept all email and attempts to filter out only those that have sender addresses recognized as those of known spammers. The invention method does not filter out unauthorized email, rather it rejects all email unless authorized. The ASL Manager in the system captures and analyzes sender and recipient usage patterns for outgoing and incoming email in order to refine the "authorized senders" lists. The analysis of this data provides a rich foundation for rules-based decisions as to which sender addresses are considered SPAMMER and which are not. This data creates

an "authorized sender" list of FRIENDS, as opposed to a list of known SPAMMERS, thereby ensuring that no unsolicited or uninvited email will ever pass through to the SUBSCRIBER's email box.

It is understood that many other modifications and variations may be devised given the above description of the guiding principles of the invention. It is intended that all such modifications and variations be considered as within the spirit and scope of this invention, as defined in the following claims.

I CLAIM:

1. A system for eliminating unauthorized email sent to a user on a network, operable with an email-receiving server (104) connected between the network and an email client (101) for receiving email addressed to a unique email address of the user, characterized by:

(a) the email-receiving server having an authorized senders list (ASL) module (203, 211) which maintains an ASL list (203b) of email addresses of senders authorized to send email to the user, and

(b) an email rejection module (202) operable with the ASL module (203) for rejecting the receipt of email addressed to the email address of the user if the email address of the sender is not one that is maintained on the ASL list for the user.

2. A system according to Claim 1, wherein the ASL module includes an ASL database (203b) for storing ASL lists of authorized sender addresses for respective subscribers of the system, a spam processor module (203) for checking the ASL lists for matches, and an ASL manager (211) for creating, maintaining, and updating the ASL lists.

3. A system according to Claim 2, wherein the email rejecting module (202) receives an email-sending message designating the sender's FROM address and intended recipient's TO address, sends a request for validation to the spam processor module to determine whether the sender's FROM address matches any authorized sender address maintained on the ASL list corresponding to the TO address of the intended recipient, accepts the email if a match to an authorized sender address is found, and rejects the email if no match to an authorized sender address is found on the ASL list.

4. A system according to Claim 3, further comprising a web-based messaging (WBM) module (204, 205) to which rejected email is redirected and which sends a message to the address of the sender to confirm that the sender is a legitimate sender of email to the intended recipient.

5. A system according to Claim 4, wherein the WBM module includes a separate web site to which the notified sender can log on and confirm that the sender is a legitimate sender of email through an interaction procedure which can only be performed by a human.

6. A system according to Claim 5, wherein the interaction procedure includes a display of a graphic image of a word in a non-standard font, and an input for the sender to enter in a word corresponding to the graphic image of the word, whereby the system can confirm that the interaction procedure is not performed by a mechanical program.

7. A system according to Claim 4, wherein once the sender is confirmed as a legitimate

sender of email to the intended recipient user, the WBM module sends the email to the user's email box with a code that indicates that the email was rejected by the redirector module but confirmed as legitimate by the WBM module.

8. A system according to Claim 3, further comprising an email-receiving manager for capturing FROM and TO addresses of accepted email and sending to the ASL manager for later analysis.

8. A system according to Claim 2, further comprising an email-sending manager for capturing FROM and TO addresses of email sent from the email client and sending to the ASL manager for later analysis.

10. A system according to Claim 2, wherein the ASL manager includes a rules processor for processing predefined address capture rules for updating the ASL lists using data from an email address source selected from the group of email address sources consisting of: received email; sent email; user inputs to email service functions on the email client; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

11. A system according to Claim 2, wherein the ASL manager includes a rules processor for processing predefined analysis rules for updating the ASL lists using data from an analysis source selected from the group of analysis sources consisting of: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

12. A system according to Claim 2, wherein the ASL manager maintains the ASL lists designating a sender-address status selected from the group of sender-address statuses consisting of: always authorized as a friend; authorized as a friend over a date range; authorized as a friend before an expiration date; always rejected as a spammer; rejected as a spammer matching a black list; and rejected as a spammer sent with an error message.

13. A method for eliminating unauthorized email sent to a user on a network addressed to a unique email address of the user, characterized by:

(a) maintaining an authorized senders list (ASL list) of email addresses of external users authorized to send email to the user, and

(b) rejecting the receipt of email sent to the email address of the user if the email address of the sender is not one maintained on the ASL list for the user.

14. A method according to Claim 13, further characterized by redirecting the rejected email to a web site for sending a message notifying the sender to confirm that the sender is a legitimate sender of email to the intended recipient.

15. A method according to Claim 14, further characterized by performing an interaction procedure at the web site with the notified sender which can only be performed by a human.

16. A method according to Claim 13, wherein maintaining the ASL list includes updating the ASL lists using data captured from any of the following sources: received email; sent email; user inputs to email service functions; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

17. A method according to Claim 13, wherein maintaining the ASL list includes updating the ASL lists using data obtained from analysis of any of the following factors: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

18. An email server system (104) for eliminating unauthorized email sent via a network addressed to a unique email address for a user of the system, characterized by:

(a) an authorized senders list (ASL) module (203, 211) which maintains an ASL list of email addresses of senders authorized to send email to the user, and

(b) an email rejection module (202) operable with the ASL module for rejecting the receipt of email addressed to the email address of the user if the email address of the sender is not one that is maintained on the ASL list for the user.

19. An email server system according to Claim 19, wherein the ASL module includes an ASL database for storing ASL lists of authorized sender addresses for respective subscribers of the system, a spam processor module for checking the ASL lists for matches, and an ASL manager for creating, maintaining, and updating the ASL lists.

20. An email server system according to Claim 19, further characterized by the email rejection module receiving an email-sending message designating the sender's FROM address and intended recipient's TO address, sending a request for validation to the spam processor module to determine whether the sender's FROM address matches any authorized sender address maintained on the ASL list corresponding to the TO address of the intended recipient, accepting the email if a match to an authorized sender address is found, and rejecting the email if no match to an authorized sender address is found on the ASL list.

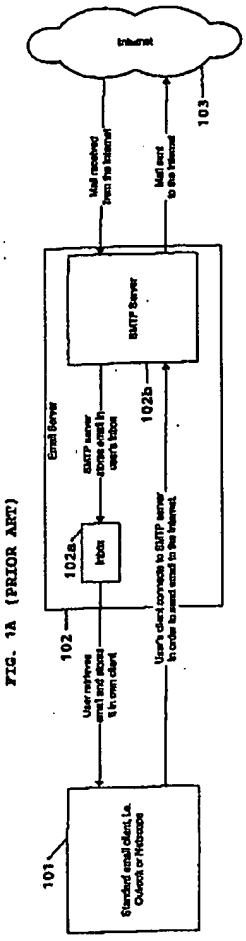


FIG. 1A (PRIOR ART)

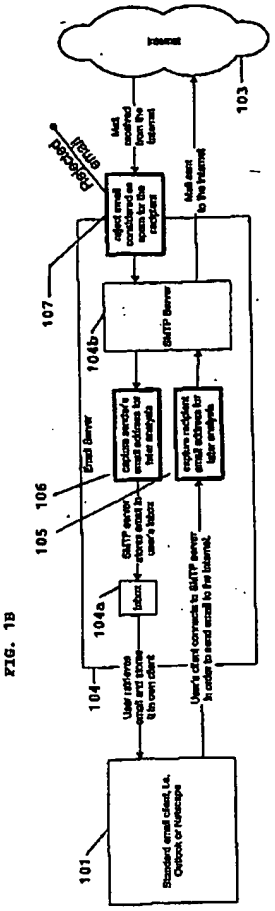


FIG. 1B

WO 01/16695 PCT/US00/23561

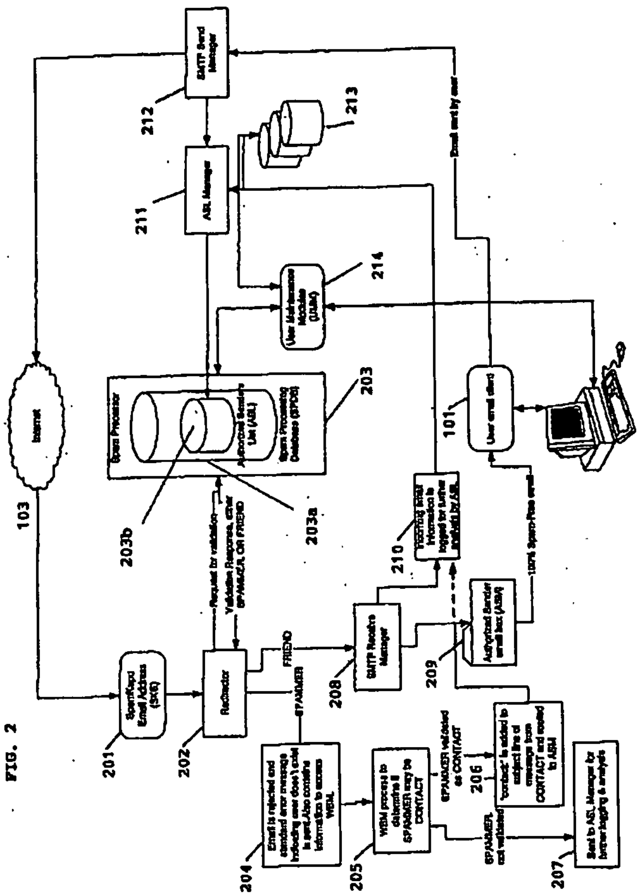


FIG. 2

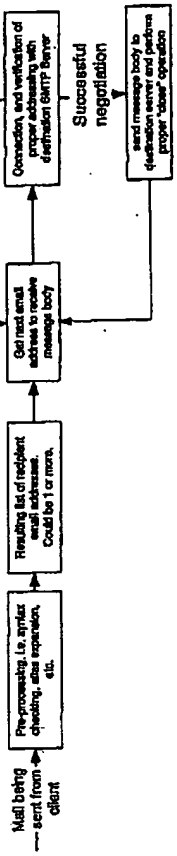


FIG. 3A (PRIOR ART)

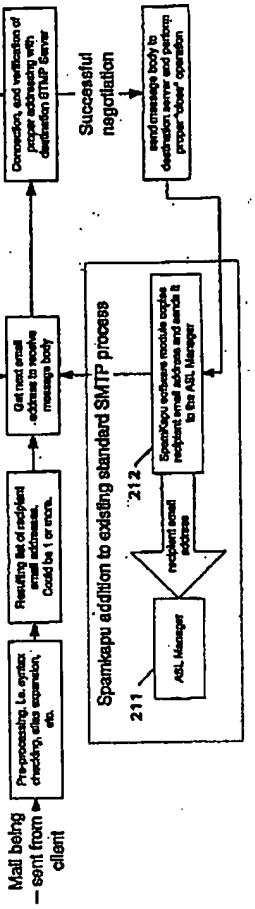


FIG. 3B

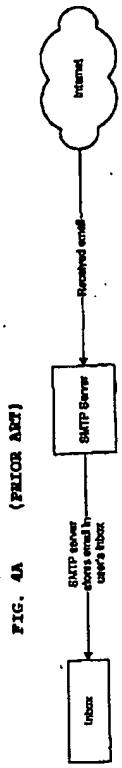


FIG. 4A (PRIOR ART)

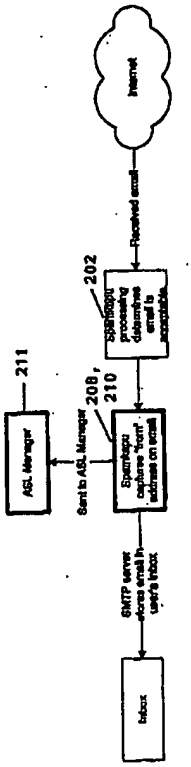


FIG. 4B

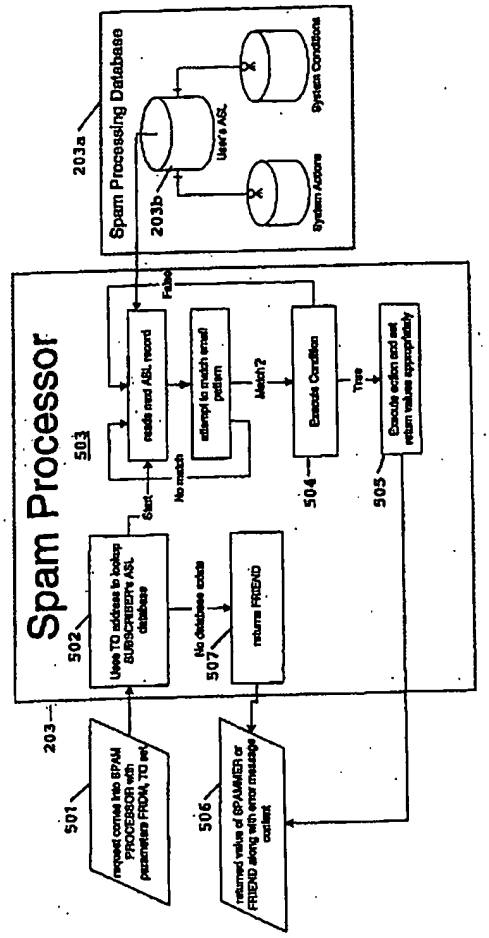
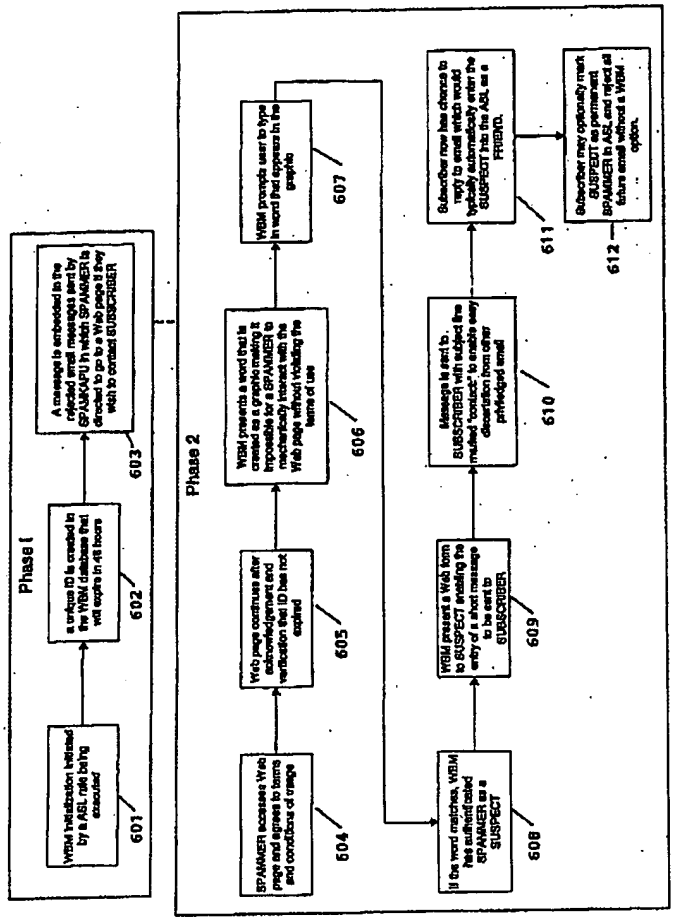

Spam Processing Database
203a
203b
User's ASL
System Conditions
System Actions
Spam Processor
503
reads next ASL record
attempt to match email pattern
Match?
Evaluate Condition
Execute action and set return values appropriately
False
No match
True
504
505
Start
Uses TO address to lookup SUBSCRIBER's ASL database
No database entries
returns FRIEND
502
507
203
request comes into SPAM PROCESSOR with parameters FROM, TO set
returned value of SPAMMER or FRIEND along with error message context
501
506

FIG. 5

FIG. 6


Phase I
WBM initialization initiated by a ABL rule being executed
601
a unique ID is created in the WBM database that will expire in 48 hours
602
A message is embedded to the rejected email messages sent by SPAMKAPU in which SPAMMER is directed to go to a Web page if they wish to contact SUBSCRIBER
603
Phase 2
SPAMMER accesses Web page and agrees to terms and conditions of usage
604
Web page continues after acknowledgement and verification that ID has not expired
605
WBM presents a word that is created as a graphic making it impossible for a SPAMMER to mechanically interact with the Web page without violating the terms of use
606
WBM prompts user to type in word that appears in the graphic
607
If the word matches, WBM flag authenticated SPAMMER as a SUSPECT
608
WBM presents a Web form to SUSPECT enabling the entry of a short message to be sent to SUBSCRIBER
609
Message is sent to SUBSCRIBER with subject line marked "conduct" to enable easy discertion from other permitted email
610
Subscriber now has chance to reply to email which would typically automatically enter the SUSPECT into the ABL as a FRIEND.
611
Subscriber may optionally mark SUSPECT as permanent SPAMMER in ABL and reject all future email without a WBM option.
612

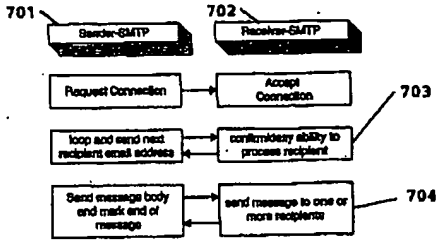

701
Sender-SMTP
702
Receiver-SMTP
Request Connection
Accept Connection
703
loop and send next recipient email address
confirm/deny ability to process recipient
Send message body and mark end of message
send message to one or more recipients
704

FIG. 7A

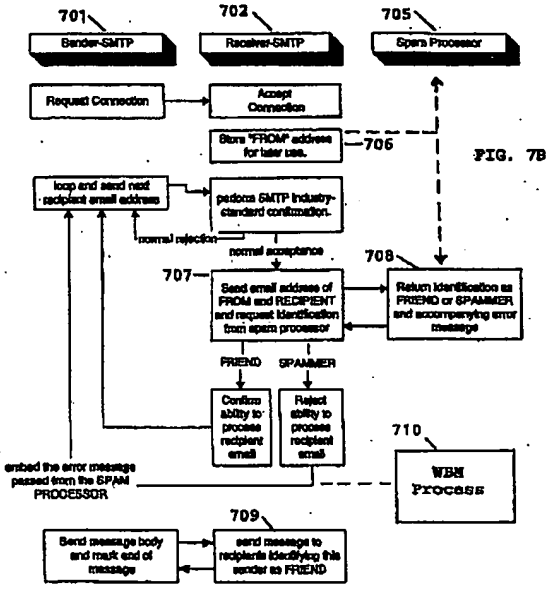

701
Sender-SMTP
702
Receiver-SMTP
705
Spam Processor
Request Connection
Accept Connection
Store "FROM" address for later use.
706
loop and send next recipient email address
pedoce SMTP industry-standard confirmation.
normal rejection
normal acceptance
708
707
Send email address of FROM and RECIPIENT and request identification from spam processor
Return identification as FRIEND or SPAMMER and accompanying error message
FRIEND
SPAMMER
Confirm ability to process recipient email
Reject ability to process recipient email
710
embed the error message passed from the SPAM PROCESSOR
WBM Process
709
Send message body and mark end of message
send message to recipients identifying this sender as FRIEND

FIG. 7B

FIG. 8

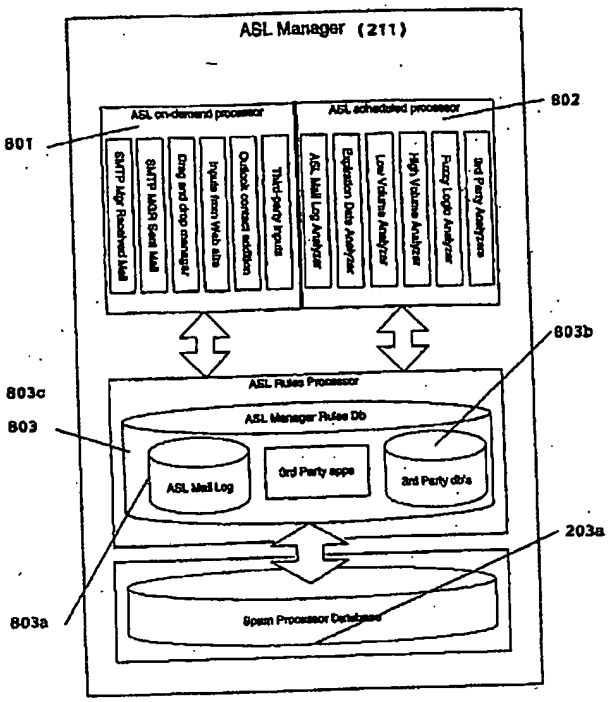
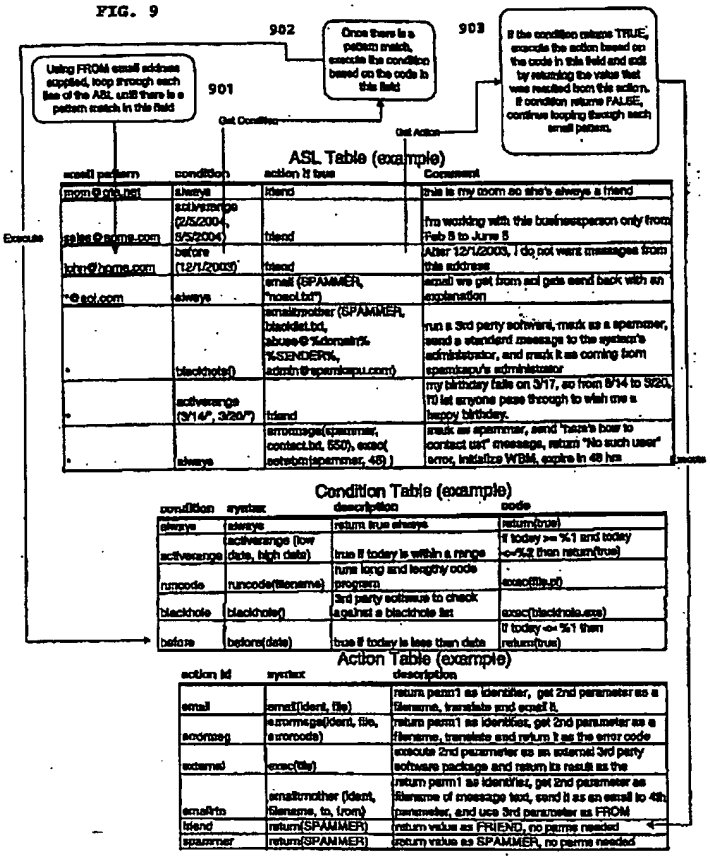

ASL Manager (211)
ASL on-demand processor
ASL scheduled processor
801
802
SMTP Mgr Received Mail
SMTP MDR Sent Mail
Drag and drop messages
Inputs from Web site
Outlook contact addition
Third-party inputs
ASL Mail Log Analyzer
Exploration Data Analyzer
Low Volume Analyzer
High Volume Analyzer
Fuzzy Logic Analyzer
3rd Party Analyzers
803b
803c
ASL Rules Processor
803
ASL Manager Rules Db
ASL Mail Log
3rd Party apps
3rd Party db's
203a
803a
Spam Processor Database

FIG. 9


902
Once there is a pattern match, execute the condition based on the code in this field
903
If the condition returns TRUE, execute the action based on the code in this field and exit by returning the value that was received from this action. If condition returns FALSE, continue looping through each email pattern.
Using FROM email address supplied, loop through each line of the ASL until there is a pattern match in this field
901
Get Condition
Get Action
Execute
ASL Table (example)
email pattern
condition
action if true
Comment
mom@ms.net
always
friend
this is my mom so she's always a friend
sales@acme.com
activerange (2/5/2004, 5/5/2004)
friend
I'm working with this businessperson only from Feb 5 to June 5
john@home.com
before (12/1/2003)
friend
After 12/1/2003, I do not want messages from this address
*@aol.com
always
email (SPAMMER, "hoaxl.txt")
email we get from aol gets send back with an explanation
*
blackhole()
emailsmother (SPAMMER, blacklist.txt, abuse@%domain% %SENDER%, admin@spamkapu.com)
run a 3rd party software, mark as a spammer, send a standard message to the system's administrator, and mark it as coming from spamkapu's administrator
*
activerange (3/14*, 3/20/*)
friend
my birthday falls on 3/17, so from 3/14 to 3/20, I'll let anyone pass through to wish me a happy birthday.
*
always
errormsg(spammer, contact.txt, 550), exec(setwbm spammer, 48))
mark as spammer, send "here's how to contact us" message, return "No such user" error, initialize WBM, expire in 48 hrs
Execute
Condition Table (example)
condition
syntax
description
code
always
always
return true always
return(true)
activerange
activerange (low date, high date)
true if today is within a range
if today >= %1 and today <=%2 then return(true)
runcode
runcode(filename)
runs long and lengthy code program
exec(file.pl)
blackhole
blackhole()
3rd party software to check against a blackhole list
exec(blackhole.exe)
before
before(date)
true if today is less than date
if today <= %1 then return(true)
Action Table (example)
action id
syntax
description
email
email(ident, file)
return parm1 as identifier, get 2nd parameter as a filename, translate and email it.
errormsg
errormsg(ident, file, errorcode)
return parm1 as identifier, get 2nd parameter as a filename, translate and return it as the error code
external
exec(file)
execute 2nd parameter as an external 3rd party software package and return its result as the
emailrtn
emailsmother (ident, filename, to, from)
return parm1 as identifier, get 2nd parameter as filename of message text, send it as an email to 4th parameter, and use 3rd parameter as FROM
friend
return(SPAMMER)
return value as FRIEND, no parms needed
spammer
return(SPAMMER)
return value as SPAMMER, no parms needed

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23361

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G 06F 7/00, 15/16, 17/00; H04N 1/00
US CL : 707/500, 709/202, 206, 209
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/500, 709/202, 206, 209

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,073,142 A (GEIGER et al) 06 June 2000, col. 5 -col. 26, lines 1-68.	1-20
Y	US 6,101,531 A (EGGLESTON et al) 08 August 2000, col. 2-col. 15, lines 1-68.	1-20
Y	US 5,944,787 A (ZOKEN) 31 August 1999, col. 2-col. 8, lines 1-68.	1-20
Y	US 6,052,709 A (PAUL) 18 April 2000, col. 3-col. 9, lines 1-68.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 OCTOBER 2000	26 DEC 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Hamod GLENTON BURGESS Telephone No. (703) 305-4792

Form PCT/ISA/210 (second sheet) (July 1998)*

フロントページの続き

(81)指定国 AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(特許庁注：以下のものは登録商標)
ＵＮＩＸ

【要約の続き】
５）に転送され、このモジュールは送信者が受信者にとって正当な電子メール送信者であることを確認するためにメッセージを送信者に送信する。もし送信者がステータスを確認するためにログオンすれば、ＷＢＭモジュールは、確認行為が機械的なプログラムによって実行されないことを保証するために人間だけが行なうことができる相互対話手続きを実行する。ＡＳＬマネージャは、送信された電子メール、受信された電子メール、ユーザによって保存されたコンタクトリスト、ユーザ優先入力、サード・パーティのプログラム等を含む様々な電子メール利用ソースの分析から収集された送信者アドレスデータに基づいたＡＳＬリストを管理する。